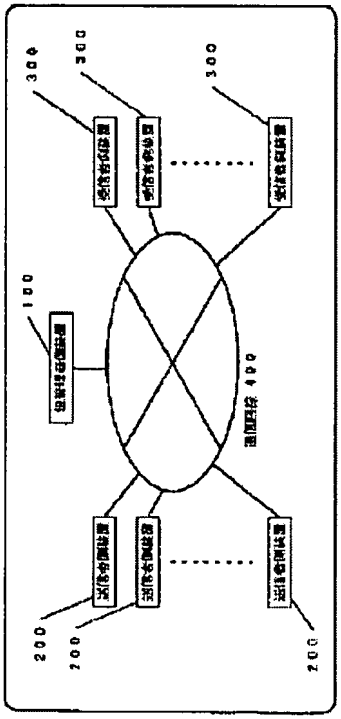
METHOD FOR DELIVERING CIPHERING AND DECIPHERING KEY IN BROADCAST CRYPTOGRAPHIC COMMUNICATION

Publication number: JP11168459
Publication date: 1999-06-22
Inventor: YAMAZAKI MASANORI; NISHIOKA GENJI; MATSUI SUSUMU
Applicant: HITACHI LTD
Classification:
- international: *G09C1/00; H04L9/08;* G09C1/00; H04L9/08; (IPC1-7): H04L9/08; G09C1/00
- European:
Application number: JP19980263498 19980917
Priority number(s): JP19980263498 19980917; JP19970271589 19971003

Abstract of **JP11168459**

PROBLEM TO BE SOLVED: To receive the delivery of each common key from plural transmitters by permitting the transmitter that distributes the third key information to obtain a ciphering/deciphering key to be used for broadcast communication by using the first key information distributed from a key manager and the third key information distributed from the transmitter. SOLUTION: This method consists of a key manager side device 100, a transmitter side device 200 and a receiver side device 300. The key manager calculates receiver identifying data of a receiver, transmits it to the transmitter, calculates transmitter key delivery data of the transmitter and transmits it to the transmitter. The transmitter calculates receiver identifying information of the receiver from one's own secrecy information, a random number and receiver identifying data of the receiver, which is receiver from the key manager, and transmits it to the receiver. Besides, the transmitter calculates receiver key delivery data so as to execute multi-address communication to the receiver. The receiver calculates a data ciphering key from key delivery data received from the transmitter, receiver identifying information, receiver secrecy information delivered from the key manage and publicized transmitter public information so as to store it in a memory.



(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（A）　(11)特許出願公開番号

特開平11－168459

(43)公開日　平成11年(1999)６月22日

(51)Int.Cl.[6]		識別記号	FI		
Ｈ０４Ｌ	9/08		Ｈ０４Ｌ	9/00	６０１Ｄ
Ｇ０９Ｃ	1/00	６３０	Ｃ０９Ｃ	1/00	６３０Ｄ
					６３０Ｅ
			Ｈ０４Ｌ	9/00	６０１Ｅ

審査請求　未請求　請求項の数25　ＯＬ　（全 33 頁）

(21)出願番号　特願平10－263498

(22)出願日　平成10年(1998)９月17日

(31)優先権主張番号　特願平9－271589

(32)優先日　平９(1997)10月３日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　山▲崎▼　正嶽
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(72)発明者　西岡　玄次
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(72)発明者　松井　進
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(74)代理人　弁理士　富田　和子

(54)【発明の名称】　同報暗号通信における暗復号化鍵の配送方法

(57)【要約】

【課題】単一の受信者秘密情報によって複数の送信者との間の共通鍵を入手可能とする。

【解決手段】鍵管理者は適当な有限集合Ｚの２個以上の元からなる部分集合に対応させて受信者の受信者秘密情報を作成し受信者に配布する。また、送信者の識別情報t_Aも作成する。送信者は自身の送信者秘密情報から暗復号化鍵K_Aを作成する。受信者秘密情報と識別情報t_Aを送信者に秘密にしながら、鍵管理者および送信者は、共同して、有限集合Ｚの各元と送信者秘密情報に関連づけたデータと、受信者秘密情報に対応する部分集合と識別情報t_Aと送信者秘密情報に関連づけたデータとを作成し、同報送信する。受信者ｘは、受信したデータと自信の受信者秘密情報から暗復号化鍵K_Aを計算する。

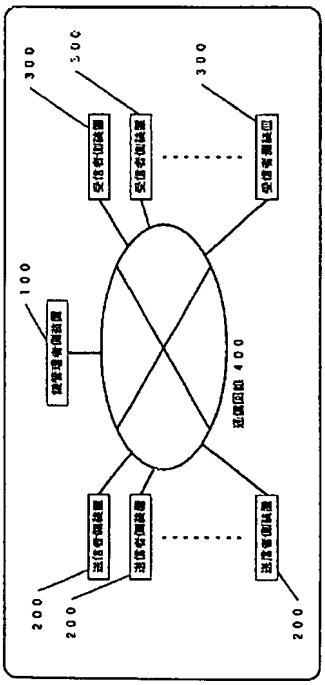


図1

【特許請求の範囲】

【請求項１】複数の送信者と 複数の受信者とが存在する通信システムにおいて、前記送信者が行う同報暗号通信の暗復号化鍵を、前記送信者と前記受信者との間で共有するための鍵配送方法であって、

鍵管理者を設け、当該鍵管理者において、前記送信者と前記受信者との間で鍵を共有するために用いる、前記複数の送信者について共通の第１鍵情報を作成し、所定の受信者に配布するとともに、前記送信者と前記受信者との間で鍵を共有するするために用いる第２鍵情報を作成し、前記送信者に配布し、

前記送信者は、受信者が前記第１鍵情報を用いて当該送信者が同報通信に用いる暗復号化鍵を算出するための第３鍵情報を、前記鍵管理者から配布された第２鍵情報を用いて生成して、当該送信者と鍵を共有する受信者に送信し、

前記受信者は、前記鍵管理者から配布された第１鍵情報と前記送信者から配布された第３鍵情報とを用いて、当該第３鍵情報を配布した送信者が同報通信に用いる暗復号化鍵を入手することを特徴とする鍵配送方法。

【請求項２】複数の送信者と 複数の受信者と、鍵管理者とが存在する通信システムを用い、前記送信者が行う同報暗号通信の暗復号化鍵を、前記送信者と前記受信者との間で共有するための鍵配送方法であって、

鍵管理者において、有限集合Ｓの部分集合Ｓ´に対応させて、受信者ｘの受信者秘密情報s_Xを作成し、当該受信者ｘに配布するとともに、送信者Ａの送信者識別情報t_Aを作成する第１ステップと、

送信者Ａにおいて、自身の送信者秘密情報G_Aを作成し、送信者秘密情報G_Aより暗復号化鍵K_Aを計算する第２ステップと、

鍵管理者と送信者Ａとが協調して、送信者秘密情報G_Aと送信者識別情報t_Aとを少なくとも作用させて鍵配送情報Ｗを作成するとともに、受信者ｘの受信者秘密鍵情報s_Xと送信者識別情報t_Aとを少なくとも作用させて、送信者Ａに対する受信者ｘの受信者識別情報r_Xを作成する第３ステップと、

送信者Ａにおいて、受信者識別情報r_Xを受信者ｘに送信し、鍵配送情報Ｗを各受信者に同報送信する第４ステップと、

受信者ｘにおいて、鍵管理者により配布された受信者秘密情報s_Xと、送信者Ａから受信した鍵配送情報Ｗおよび受信者識別情報r_Xとから、送信者Ａが行う同報暗号通信の暗復号化鍵K_Aを算出する第５ステップと、を有し、

前記受信者秘密情報s_X、鍵配送情報Ｗ、および受信者識別情報r_Xは、前記受信者秘密情報s_X、鍵配送情報Ｗ、および受信者識別情報r_Xと各受信者に公開される他の情報とより、暗復号化鍵K_Aが導出可能な関係をもって作成されることを特徴とする鍵配送方法。

【請求項３】請求項２記載の鍵配送方法であって、

前記第２ステップにおいて、送信者Ａは、暗復号化鍵を変更するための変数情報r_A，r_A'を作成し、送信者秘密情報G_Aに変数情報r_A，r_A'を作用させて、暗復号化鍵K_Aを計算し、

前記第３ステップにおいて、鍵管理者は、送信者秘密情報G_Aと送信者識別情報t_Aとを作用させたデータＷ´を作成して送信者Ａに送信するとともに、受信者ｘの受信者秘密情報s_Xと送信者識別情報t_Aとを作用させたr_X´を作成して、送信者Ａに送信し、かつ、送信者Ａは、データＷ´に変数情報r_Aを作用させて鍵配送情報Ｗを作成し、データr_X´に変数情報r_A´を作用させて送信者Ａに対する受信者ｘの受信者識別情報r_Xを作成することを特徴とする鍵配送方法。

【請求項４】複数の送信者と 複数の受信者と、鍵管理者とが存在する通信システムを用い、前記送信者が行う同報暗号通信の暗復号化鍵を、前記送信者と前記受信者との間で共有するための鍵配送方法であって、

鍵管理者において、鍵管理者秘密情報として、

【数１】

数1

$$e_i \in Z, \quad (1 \leq i \leq m)$$

を作成し、送信者Ａの送信者識別情報として、

【数２】

数2

$$t_A \in Z$$

を作成し、受信者ｘの受信者秘密情報として、$\sigma_X \in S_{km}$と、

【数３】

数3

$$s_x(\sigma_x) \in Z$$

（但し、集合

【数４】

数4

$$S_{km} = \{\sigma \mid 1\text{対}1\text{写像}\ \sigma : A = \{1, 2, \cdots, k\} \to B = \{1, 2, \cdots, m\}, 0 < k < m\}$$

に対して、σ、σ' $\in S_{km}$のとき

【数５】

数5

$$\sigma \sim \sigma' \quad \overset{\text{def}}{\Longleftrightarrow} \quad \sigma(A) = \sigma'(A)$$

とし、このとき、～はS_{km}上の同値関係となり、

【数6】

数6

$$\tilde{S}_{km} = S_{km} / \sim$$

とする）とを作成し、受信者秘密情報σ_X、$s_X(\sigma_X)$を受信者xに配布するステップと、
送信者Aにおいて、
【数7】

数7

- $g_A \in G_A$
- $L_A = \mathrm{ord}_{G_A}(g_A)$

（但し、
【数8】

数8

$$\mathrm{ord}_{G_A}(g)$$

は、
【数9】

数9

$$g^a = 1 \ (\in G_A)$$

なる最小の正整数aを表す）なる送信者秘密情報g_A、L_Aおよび有限アーベル群G_Aを作成し、送信者秘密情報g_Aを鍵管理者に送信するステップと、
鍵管理者において、鍵管理者秘密情報e_i、送信者識別情報t_Aおよび受信者秘密情報$s_X(\sigma_X)$、σ_Xから、受信者識別データ
【数10】

数10

$$s_x(\sigma_x, A) = t_A s_x(\sigma_x) \sum_{i=1}^{k} e_{\sigma_x(i)}$$

を計算して、受信者識別データ$s_X(\sigma_X, A)$を送信者Aに送信するとともに、送信者Aから受信したg_Aと、鍵管理者秘密情報e_iと、送信者識別情報t_Aから、鍵配送データ
【数11】

数11

$$y_{Ai} = g_A^{t_A e_i} \ (\in G_A) \quad (1 \le i \le m)$$

を算出して、鍵配送データy_{Ai}を送信者Aに送信するステップと、
送信者Aにおいて、整数r、r´を生成し、鍵管理者から受信した受信者識別データ$s_X(\sigma_X, A)$と、送信者秘密情報L_Aと、整数r´から

【数12】

数12

$$r_x(\sigma_x, A) s_x(\sigma_x, A) \equiv r' \pmod{L_A}$$

なる受信者識別情報$r_X(\sigma_X, A)$を計算して、受信者識別情報$r_X(\sigma_X, A)$を受信者xに送信するとともに、鍵管理者から受信した鍵配送データy_{Ai}と、整数rから、鍵配送情報
【数13】

数13

$$z_{Ai} = y_{Ai}^{r} \ (\in G_A) \quad (1 \le i \le m)$$

を計算し、鍵配送情報z_{Ai}を、各受信者に同報送信するステップと、
受信者xにおいて、送信者から受信した受信者識別情報$r_X(\sigma_X, A)$および鍵配送情報z_{Ai}と、鍵管理者から配布された受信者秘密情報σ_X、$s_X(\sigma_X)$から、
【数14】

数14

$$K_A = \left(\prod_{i=1}^{k} z_{A\sigma_x(i)} \right)^{r_x(\sigma_x, A) s_x(\sigma_x)} \ (\in G_A)$$

により、送信者Aが
【数15】

数15

$$K_A = g_A^{r'} \ (\in G_A)$$

によって生成し、同報通信に用いる暗復号化鍵K_Aを計算するステップと、を有することを特徴とする鍵配送方法。
【請求項5】複数の送信者と 複数の受信者と、鍵管理者とが存在する通信システムを用い、前記送信者が行う同報暗号通信の暗復号化鍵を、前記送信者と前記受信者との間で共有するための鍵配送方法であって、
鍵管理者において、鍵管理者秘密情報として、
【数16】

数16

$$e_i \in Z \ (1 \le i \le m)$$

を作成し、送信者Aの送信者識別情報として、
【数17】

数17

$$t_A \in Z$$

を作成し、受信者xの受信者秘密情報として、$\sigma_X \in S_{km}$と、
【数18】

数18

$$s_x(\sigma_x) \in Z$$

数19

$$S_{km} = \{\sigma \mid 1\text{対}1\text{写像}\ \sigma : A = \{1,2,\cdots,k\} \to B = \{1,2,\cdots,m\}, 0 < k < m\}$$

に対して、σ、σ´∈S_{km}のとき

【数20】

数20

$$\sigma \sim \sigma' \quad \overset{\text{def.}}{\Longleftrightarrow} \quad \sigma(A) = \sigma'(A)$$

とし、このとき、～はS_{km}上の同値関係となり、

【数21】

数21

$$\tilde{S}_{km} = S_{km} / \sim$$

数22

$$P_A, Q_A : \text{素数}$$

$$L_A = \mathrm{lcm}(\mathrm{ord}_{P_A}(g_A), \mathrm{ord}_{Q_A}(g_A))$$

$$g_A \in Z, 0 < g_A < N_A$$

を作成し、送信者Aの送信者公開情報として、

【数23】

数23

$$N_A (= P_A Q_A)$$

を作成し、送信者秘密情報g_Aを鍵管理者に送信するステップと、

鍵管理者において、鍵管理者秘密情報e_i、送信者識別情報t_Aおよび受信者秘密情報$s_X(\sigma_X)$、σ_Xから、受信者識別データ

【数24】

数24

$$s_x(\sigma_x, A) = t_A s_x(\sigma_x) \sum_{i=1}^{k} e_{\sigma_x(i)}$$

を計算し、受信者識別データ$s_X(\sigma_X, A)$を送信者Aに送信し、送信者Aから受信したg_Aと、鍵管理者秘密情報e_iと、送信者識別情報t_Aから、鍵配送データ

【数25】

数25

$$y_{Ai} = g_A^{t_A e_i} \mod N_A \quad (1 \le i \le m)$$

を算出し、鍵配送データy_{Ai}を送信者Aに送信するステップと、

送信者Aにおいて、整数r、r´を生成し、鍵管理者から受信した受信者識別データ$s_X(\sigma_X, A)$と、送信者秘密情報L_Aと、整数r´から

【数26】

数26

$$r_x(\sigma_x, A) s_x(\sigma_x, A) \equiv r' \pmod{L_A}$$

なる受信者識別情報$r_X(\sigma_X, A)$を計算し、受信者識別情報$r_X(\sigma_X, A)$を受信者xに送信するとともに、鍵管理者から受信した鍵配送データy_{Ai}と整数rから、鍵配送情報

【数27】

数27

$$z_{Ai} = y_{Ai}{}^{r} \bmod N_A \quad (1 \le i \le m)$$

を計算し、鍵配送情報z_{Ai}を、各受信者に同報送信するステップと、

（但し、集合

受信者xにおいて、送信者から受信した受信者識別情報$r_X(\sigma_X, A)$および鍵配送情報z_{Ai}と、鍵管理者から配布された受信者秘密情報σ_X、$s_X(\sigma_X)$から

【数28】

数28

$$K_A = \left(\prod_{i=1}^{k} z_{A\sigma_x(i)} \right)^{r_x(\sigma_x, A) s_x(\sigma_x)} \mod N_A$$

により、送信者Aが

【数29】

数29

$$K_A = g_A^{r'} \mod N_A$$

によって生成し同報通信に用いる暗復号化鍵K_Aを計算するステップと、を有することを特徴とする鍵配送方法。

【請求項6】請求項4または5記載の鍵配送方法であって、

送信者Aは、鍵管理者が、前記鍵管理者秘密情報e_i、送信者識別情報t_A、受信者秘密情報$s_X(\sigma_X)$を生成するのに先だって、前記秘密情報L_Aを生成して鍵管理者に送信し、

鍵管理者は、前記鍵管理者秘密情報e_i、送信者識別情報t_A、受信者秘密情報$s_X(\sigma_X)$として、送信者から受信した送信者秘密情報L_Aから

【数30】

数30

$$e_i \in Z, \quad 0 < e_i < L_A, \quad (1 \le i \le m)$$

$$t_A \in Z, \quad 0 < t_A < L_A$$

$$s_x(\sigma_x) \in Z, \quad 0 < s_x(\sigma_x) < L_A$$

となる鍵管理者秘密情報e_i、送信者識別情報t_A、受信者秘密情報$s_X(\sigma_X)$を作成し、前記受信者識別データ$s_X(\sigma_X, A)$として、送信者秘密情報L_A、鍵管理者秘密情報e_i、送信者識別情報t_A、受信者秘密情報$s_X(\sigma_X)$から

【数31】

数31

$$s_x(\sigma_x, A) = t_A s_x(\sigma_x) \sum_{i=1}^{k} e_{\sigma_x(i)} \mod L_A$$

に従った受信者識別データ$s_X(\sigma_X, A)$を計算することを特徴とする鍵配送方法。

【請求項7】請求項4または5記載の鍵配送方法であって、さらに、

送信者Aにおいて、前記整数rの値を変更し、変更後の整数rに従って、暗復号化鍵K_Aの値を再計算し、変更後の整数rに従って、鍵配送情報z_{Ai}を再計算して各受信者に、再同報送信するステップと、

受信者xにおいて、再同報送信された鍵配送情報z_{Ai}に従って、暗復号化鍵K_Aを再計算するステップと、を有することを特徴とする鍵配送方法。

【請求項8】請求項4または5記載の鍵配送方法であって、

送信者Aは、前記整数r'の値を、暗号化して同報通信する情報もしくは情報の種類の各々に対応して生成し、前記情報もしくは情報の種類毎に、当該情報もしくは情報の種類に対応して生成した整数r'の各々に従って、各々暗復号化鍵K_Aを計算し、受信者xに復号化を許可する前記情報もしくは情報の種類に対応して生成した各整数r'の各々に従って、受信者識別情報$r_X(\sigma_X, A)$を各々計算して当該受信者xに送信し、

受信者xは、受信した各受信者識別情報$r_X(\sigma_X, A)$に従って、当該受信者xに復号化が許可された前記情報もしくは情報の種類各々の暗復号化鍵K_Aを各々計算することを特徴とする鍵配送方法。

【請求項9】請求項4または5記載の鍵配送方法であって、

送信者Aが、受信者xであることを主張する受信者に受信者識別情報$r_X(\sigma_X, A)$を送信するのに先だって、当該受信者が、受信者秘密情報$s_X(\sigma_X)$を所持していることを、当該受信者が受信者xである場合にも受信者秘密情報$s_X(\sigma_X)$が送信者Aに秘密化される方式によって認証するステップを備えたことを特徴とする鍵配送方法。

【請求項10】請求項4、5または9記載の鍵配送方法であって、

送信者Aにおいて、受信者xに受信者識別情報$r_X(\sigma_X, A)$を送信する際に、当該受信者識別情報$r_X(\sigma_X, A)$に対応する暗復号化鍵K_Aによって暗号化されて同報通信される情報もしくは情報の種類に対する料金を、受信者Aに対する課金情報として算出するステップを有することを特徴とする鍵配送方法。

【請求項11】複数の送信者と、複数の受信者とが存在する通信システムにおいて、前記送信者が行う同報暗号通信の暗復号化鍵を、前記送信者と前記受信者との間で共有するための鍵配送方法であって、

鍵管理者を設け、当該鍵管理者において、秘密情報K0を生成し、各送信者と各受信者に配布するステップと、

送信者Ａにおいて、送信者識別情報BID_Aを生成して受信者に送信するとともに、鍵管理者から配布された秘密情報Ｋ０と送信者識別情報BID_Aから、所定の一方向性関数Ｆにより、共有鍵$K_A^{-}=F(K0, BID_A)$を計算するステップと、
受信者において、鍵管理者から配布された秘密情報Ｋ０と送信者Ａから受信した送信者識別情報BID_Aから、前記一方向性関数Ｆにより、共有鍵K_A^{-}を計算するステップと、
送信者Ａにおいて、整数ｒを作成して受信者に送信するステップと、
受信者において、送信者Ａから受信した整数ｒと共有鍵K_A^{-}から、所定の関数F^{-}により、送信者Ａにおいて$K_A=F^{-}(r, K_A^{-})$によって計算される暗復号化鍵K_Aを、$K_A=F^{-}(r, K_A^{-})$によって計算するステップと、を備えたことを特徴とする鍵配送方法。

【請求項１２】複数の送信者と 複数の受信者とが存在する通信システムにおいて、前記送信者が行う同報暗号通信の暗復号化鍵を、前記送信者と前記受信者との間で共有するための鍵配送方法であって、
鍵管理者を設け、当該鍵管理者において、受信者ｘの個別鍵s_Xを作成して、送信者Ａと受信者ｘに配布するステップと、
送信者Ａにおいて、共有鍵K_Aを作成し、鍵管理者から配布された受信者ｘの個別鍵s_Xを使った暗号通信により、共有鍵K_Aを受信者ｘと共有するステップと、
送信者Ａにおいて、情報ｒを作成し、受信者ｘに送信するステップと、
受信者ｘおよび送信者Ａにおいて、暗復号化鍵ＤＫを、$DK=F(r, K_A)$に従って各々計算するステップと、を備えたことを特徴とする鍵配送方法。

【請求項１３】請求項１２記載の鍵配送方法であって、
送信者Ａにおいて、共有鍵K_Aを変更し、変更した共有鍵K_Aを、受信者ｘの個別鍵s_Xを使った暗号通信により受信者ｘと共有するステップと、
送信者Ａおよび受信者ｘにおいて、暗復号化鍵ＤＫを、変更した共有鍵K_Aにを用いて、$DK=F(r, K_A)$により再計算するステップと、を備えたことを特徴とする鍵配送方法。

【請求項１４】請求項１２記載の鍵配送方法であって、
送信者Ａにおいて、情報ｒを変更し、変更した情報ｒを受信者に伝えるステップと、
送信者Ａおよび受信者ｘにおいて、暗復号化鍵ＤＫを、変更後の情報ｒを用いて、$DK=F(r, K_A)$により再計算するステップと、を備えたことを特徴とする鍵配送方法。

【請求項１５】請求１、２、３、１１または１２記載の鍵配送方法であって、
送信者Ａは、暗復号化鍵により情報を暗号化して同報通信する通信チャネルとは異なる所定の通信チャネルを用いて、受信者ｘが送信者Ａとの間で共有する暗復号化鍵を算出するための鍵情報を送信するステップを備えたことを特徴とする鍵配送方法。

【請求項１６】同報暗号通信を行う通信システムにおいて、同報暗号通信に用いる暗復号化鍵を、送信者と受信者との間で共有するための鍵配送システムであって、
鍵管理者装置と、複数の送信者装置と、複数の受信者装置とを含み、
前記鍵管理者装置は、
鍵管理者秘密情報として、
【数３２】

数32

$$e_i \in Z, \quad (1 \le i \le m)$$

を作成し、送信者Ａの送信者識別情報として、
【数３３】

数33

$$\bullet\ t_A \in Z$$

を作成し、受信者ｘの受信者秘密情報として、$\sigma_X \in S_{km}$と、
【数３４】

数34

$$\bullet\ s_x(\sigma_x) \in Z$$

（但し、集合
【数３５】

数35

$$S_{km} = \{\sigma \mid 1\text{対}1\text{写像}\ \sigma : A = \{1, 2, \cdots, k\} \to B = \{1, 2, \cdots, m\}, 0 < k < m\}$$

に対して、σ、$\sigma^{-} \in S_{km}$のとき、
【数３６】

数36

$$\sigma \sim \sigma' \quad \overset{\text{def}}{\Longleftrightarrow} \quad \sigma(A) = \sigma'(A)$$

とし、このとき、～はS_{km}上の同値関係となり、
【数３７】

数37

$$\tilde{S}_{km} = S_{km} / \sim$$

とする）とを作成し、受信者秘密情報σ_X、$s_X(\sigma_X)$を受信者ｘが使用する受信者装置ｘに配布する手段と、鍵管理者秘密情報e_i、送信者識別情報t_Aおよび受信者

秘密情報$s_X(\sigma_X)$、σ_Xから、受信者識別データ

【数38】

数38

$$s_x(\sigma_x, A) = t_A s_x(\sigma_x) \sum_{i=1}^{k} c_{\sigma_x(i)}$$

を計算して、受信者識別データ$s_X(\sigma_X, A)$を送信者Aが使用する送信者装置Aに送信するとともに、前記送信者装置Aから受信したg_Aと、鍵管理者秘密情報e_iと、送信者識別情報t_Aから、鍵配送データ

【数39】

数39

$$y_{Ai} = g_A^{t_A e_i} \ (\in G_A) \quad (1 \leq i \leq m)$$

を算出し、鍵配送データy_{Ai}を前記送信者装置Aに送信する手段と、を有し、

前記送信者装置Aは、

【数40】

数40

- $g_A \in G_A$
- $L_A = \mathrm{ord}_{G_A}(g_A)$

（但し、

【数41】

数41

$$\mathrm{ord}_{G_A}(g)$$

は、

【数42】

数42

$$g^a = 1 \ (\in G_A)$$

なる最小の正整数aを表す）なる送信者秘密情報g_A、L_Aおよび有限アーベル群G_Aを作成し、送信者秘密情報g_Aを前記鍵管理者装置に送信する手段と、

整数r、r´を生成し、前記鍵管理者装置から受信した受信者識別データ$s_X(\sigma_X, A)$と、送信者秘密情報L_Aと、整数r´から

【数43】

数43

$$r_x(\sigma_x, A) s_x(\sigma_x, A) \equiv r' \pmod{L_A}$$

なる受信者識別情報$r_X(\sigma_X, A)$を計算し、受信者識別情報$r_X(\sigma_X, A)$を前記受信者装置xに送信するとともに、前記鍵管理者装置から受信した鍵配送データy_{Ai}と、整数rから、鍵配送情報

【数44】

数44

$$z_{Ai} = y_{Ai}^{r} \ (\in G_A) \quad (1 \leq i \leq m)$$

を計算し、鍵配送情報z_{Ai}を、前記複数の受信者装置に同報送信する手段と、を有し、

前記受信者装置xは、

前記送信者装置Aから受信した受信者識別情報$r_X(\sigma_X, A)$および鍵配送情報z_{Ai}と、前記鍵管理者装置から配布された受信者秘密情報σ_X、$s_X(\sigma_X)$から、

【数45】

数45

$$K_A = \left(\prod_{i=1}^{k} z_{A\sigma_x(i)} \right)^{r_x(\sigma_x, A) s_x(\sigma_x)} \ (\in G_A)$$

により、前記送信者装置Aが

【数46】

数46

$$K_A = g_A^{rr'} \ (\in G_A)$$

によって生成し、同報通信に用いる暗復号化鍵K_Aを計算する手段と、を有することを特徴とする通信システム。

【請求項17】同報暗号通信を行う複数の送信者装置と、複数の受信者装置と、前記送信者装置が同報暗号通信に用いる暗復号化鍵の前記受信者装置への配送を支援する鍵管理者装置とを有する通信システムに用いられる鍵管理者装置であって、

鍵管理者秘密情報として、

【数47】

数47

$$e_i \in \mathbb{Z}, \quad (1 \leq i \leq m)$$

を作成し、送信者Aの送信者識別情報として、

【数48】

数48

$$t_A \in \mathbb{Z}$$

を作成し、受信者xの受信者秘密情報として、$\sigma_X \in S_{km}$と、

【数49】

数49

$$s_x(\sigma_x) \in \mathbb{Z}$$

（但し、集合

【数50】

数50

$$S_{km} = \{\sigma \mid 1\text{対}1\text{写像}\ \sigma : A = \{1, 2, \cdots, k\} \to B = \{1, 2, \cdots, m\}, 0 < k < m\}$$

に対して、σ、σ´∈S_{km}のとき

【数５１】

数51

$$\sigma \sim \sigma' \quad \overset{\text{def}}{\Longleftrightarrow} \quad \sigma(A) = \sigma'(A)$$

とし、このとき、～はS_{km}上の同値関係となり、

【数５２】

数52

$$\tilde{S}_{km} = S_{km} / \sim$$

とする）とを作成し、受信者秘密情報σ_X、s_X（σ_X）を受信者ｘが使用する受信者装置ｘに配布する手段と、鍵管理者秘密情報e_i、送信者識別情報t_Aおよび受信者秘密情報s_X（σ_X）、σ_Xから、受信者識別データ

【数５３】

数53

$$s_x(\sigma_x, A) = t_A s_x(\sigma_x) \sum_{i=1}^{k} e_{\sigma_x(i)}$$

を計算し、受信者識別データs_X（σ_X，Ａ）を送信者Ａが使用する送信者装置Ａに送信するとともに、前記送信者装置Ａから受信したg_Aと、鍵管理者秘密情報e_iと、送信者識別情報t_Aから、鍵配送データ

【数５４】

数54

$$y_{Ai} = g_A^{t_A e_i} \ (\in G_A) \quad (1 \le i \le m)$$

を算出し、鍵配送データy_{Ai}を前記送信者装置Ａに送信する手段と、を有することを特徴とする鍵管理者装置。

【請求項１８】同報暗号通信を行う複数の送信者装置と、複数の受信者装置と、前記送信者装置が同報暗号通信に用いる暗復号化鍵の前記受信者装置への配送を支援する鍵管理者装置とを有する通信システムに用いられる送信者装置であって、

【数５５】

数55

$$g_A \in G_A$$

$$L_A = \mathrm{ord}_{G_A}(g_A)$$

（但し、

【数５６】

数56

$$\mathrm{ord}_{G_A}(g)$$

は、

【数５７】

数57

$$g^a = 1 \ (\in G_A)$$

なる最小の正整数ａを表す）なる送信者秘密情報g_A、L_Aおよび有限アーベル群G_Aを作成し、送信者秘密情報g_Aを前記鍵管理者装置に送信する手段と、

整数ｒ、ｒ´を生成し、前記鍵管理者装置から受信した受信者識別データs_X（σ_X，Ａ）と、送信者秘密情報L_Aと、整数ｒ´から

【数５８】

数58

$$r_x(\sigma_x, A) s_x(\sigma_x, A) \equiv r' \pmod{L_A}$$

なる受信者識別情報r_X（σ_X，Ａ）を計算し、受信者識別情報r_X（σ_X，Ａ）を受信者ｘが使用する受信者装置ｘに送信するとともに、前記鍵管理者装置から受信した鍵配送データy_{Ai}と、整数ｒから、鍵配送情報

【数５９】

数59

$$z_{Ai} = y_{Ai}^{r} \ (\in G_A) \quad (1 \le i \le m)$$

を計算し、鍵配送情報z_{Ai}を、前記複数の受信者装置に同報送信する手段と、

【数６０】

数60

$$K_A = g_A^{r'} \ (\in G_A)$$

に従って同報通信に用いる暗復号化鍵K_Aを計算する手段と、を有することを特徴とする送信者装置。

【請求項１９】同報暗号通信を行う複数の送信者装置と、複数の受信者装置と、前記送信者装置が同報暗号通信に用いる暗復号化鍵の前記受信者装置への配送を支援する鍵管理者装置とを有する通信システムに用いられる受信者装置であって、

送信者Ａが使用する送信者装置Ａから受信した受信者識別情報r_X（σ_X，Ａ）および鍵配送情報z_{Ai}と、前記鍵管理者装置から配布された受信者秘密情報σ_X、s_X（σ

$_X$）から
【数６１】
数61

$$K_A = \left(\prod_{i=1}^{k} z_{A\sigma_x(i)} \right)^{r_x(\sigma_x, A) s_x(\sigma_x)} \quad (\in G_A)$$

により、前記送信者装置Ａが
【数６２】
数62

$$K_A = g_A^{rr'} \quad (\in G_A)$$

によって生成し、同報通信に用いる暗復号化鍵K_Aを計算する手段と、を有することを特徴とする受信者装置。
【請求項２０】同報暗号通信を行う複数の送信者装置と、複数の受信者装置と、前記送信者装置が同報暗号通信に用いる暗復号化鍵の前記受信者装置への配送を支援する鍵管理者装置とを有する通信システムに用いられる受信者装置であって、
本体装置と、補助装置とを有し、
前記補助装置は、
前記鍵管理者装置と接続する手段と、
前記鍵管理者装置が作成した受信者秘密情報$s_X(\sigma_X)$、σ_Xを取り込んで記憶する記憶手段と、
前記本体装置に接続する手段と、
前記本体装置が送信者Ａの使用する送信者装置Ａから受信した鍵配送情報z_{Ai}を取り込み、鍵配送情報z_{Ai}と、前記記憶手段に記憶した受信者秘密情報σ_X、$s_X(\sigma_X)$から、
【数６３】
数63

$$\xi_x(\sigma_x, A) = \left(\prod_{i=1}^{k} z_{A\sigma_x(i)} \right)^{s_x(\sigma_x)} \bmod N_A$$

を計算して、計算結果$\xi_X(\sigma_X, A)$を前記本体装置に出力する手段と、を備え、
前記本体装置は、
前記送信者装置Ａから受信した鍵配送情報z_{Ai}を前記補助装置に出力する手段と、
前記送信者装置Ａから受信した受信者識別情報$r_X(\sigma_X, A)$と、前記補助装置が出力した$\xi_X(\sigma_X, A)$から、
【数６４】
数64

$$K_A = \xi_x(\sigma_x, A)^{r_x(\sigma_x, A)} \bmod N_A$$

に従って、前記送信者装置Ａが
【数６５】
数65

$$K_A = g_A^{rr'} \quad (\in G_A)$$

によって生成し、同報通信に用いる暗復号化鍵K_Aを計算する手段と、を備えていることを特徴とする受信者装置。
【請求項２１】同報通信を行う複数の送信者装置と、複数の受信者装置と、前記送信者装置が同報暗号通信に用いる暗復号化鍵の前記受信者装置への配送を支援する鍵管理者装置とを有する通信システムにおいて、前記鍵管理者装置および前記受信者装置に接続して用いられる補助装置であって、
前記鍵管理者装置と接続する手段と、
前記鍵管理者装置が作成した受信者ｘの受信者秘密情報$s_X(\sigma_X)$、σ_Xを取り込んで記憶する記憶手段と、
受信者ｘの使用する受信者装置ｘに接続する手段と、
前記受信者装置ｘが送信者Ａの使用する送信者装置Ａから受信した鍵配送情報z_{Ai}を取り込み、鍵配送情報z_{Ai}と、前記記憶手段に記憶した受信者秘密情報σ_X、$s_X(\sigma_X)$から、
【数６６】
数66

$$\xi_x(\sigma_x, A) = \left(\prod_{i=1}^{k} z_{A\sigma_x(i)} \right)^{s_x(\sigma_x)} \bmod N_A$$

を計算して、計算結果$\xi_X(\sigma_X, A)$を前記受信者装置ｘに出力する手段と、を備えていることを特徴とする補助装置。
【請求項２２】同報暗号通信を行う複数の送信者装置と、複数の受信者装置と、前記送信者装置が同報暗号通信に用いる暗復号化鍵の前記受信者装置への配送を支援する鍵管理者装置とを有する通信システムにおいて、前記鍵管理者装置における処理をコンピュータに実行させるプログラムを記憶した記憶媒体であって、
当該プログラムは、コンピュータに、
鍵管理者秘密情報として、
【数６７】
数67

$$e_i \in \mathbb{Z}, \quad (1 \leq i \leq m)$$

を作成し、送信者Ａの送信者識別情報として、
【数６８】
数68

$$t_A \in \mathbb{Z}$$

を作成し、受信者ｘの受信者秘密情報として、$\sigma_X \in S_{km}$と、
【数６９】

数69

$$s_x(\sigma_x) \in \mathbb{Z}$$

数70

$$S_{km} = \{\sigma \mid 1\text{対}1\text{写像}\ \sigma : A = \{1, 2, \cdots, k\} \to B = \{1, 2, \cdots, m\}, 0 < k < m\}$$

に対して、σ、σ´∈S_{km}のとき

【数７１】

数71

$$\sigma \sim \sigma' \quad \overset{\text{def}}{\Longleftrightarrow} \quad \sigma(A) = \sigma'(A)$$

とし、このとき、～はS_{km}上の同値関係となり、

【数７２】

数72

$$\tilde{S}_{km} = S_{km} / \sim$$

とする）とを作成し、受信者秘密情報σ_X、s_X（σ_X）を受信者xが使用する受信者装置xに配布する手順と、鍵管理者秘密情報e_i、送信者識別情報t_Aおよび受信者秘密情報s_X（σ_X）、σ_Xから、受信者識別データ

【数７３】

数73

$$s_x(\sigma_x, A) = t_A s_x(\sigma_x) \sum_{i=1}^{k} e_{\sigma_x(i)}$$

を計算して、受信者識別データs_X（σ_X，Ａ）を送信者Ａが使用する送信者装置Ａに送信するとともに、前記送信者装置Ａから受信したg_Aと、鍵管理者秘密情報e_iと、送信者識別情報t_Aから、鍵配送データ

【数７４】

数74

$$y_{Ai} = y_A^{t_A \sigma_i} \ (\in G_A) \quad (1 \leq i \leq m)$$

を算出し、鍵配送データy_{Ai}を前記送信者装置Ａに送信する手順と、を実行させることを特徴とするプログラムが記憶された記憶媒体。

【請求項２３】同報暗号通信を行う複数の送信者装置と、複数の受信者装置と、前記送信者装置が同報暗号通信に用いる暗復号化鍵の前記受信者装置への配送を支援する鍵管理者装置とを有する通信システムにおいて、前記送信者装置における処理をコンピュータに実行させるプログラムを記憶した記憶媒体であって、

当該プログラムは、コンピュータに、

【数７５】

数75

$$g_A \in G_A$$

$$L_A = \mathrm{ord}_{G_A}(g_A)$$

（但し、

【数７６】

数76

$$\mathrm{ord}_{G_A}(g)$$

は、

【数７７】

数77

$$g^a = 1 \ (\in G_A)$$

なる最小の正整数ａを表す）なる送信者秘密情報g_A、L_Aおよび有限アーベル群G_Aを作成し、送信者秘密情報g_Aを前記鍵管理者装置に送信する手順と、

整数ｒ、ｒ´を生成し、前記鍵管理者装置から受信した受信者識別データs_X（σ_X，Ａ）と、送信者秘密情報L_Aと、整数ｒ´から、

【数７８】

数78

$$r_x(\sigma_x, A) s_x(\sigma_x, A) \equiv r' \pmod{L_A}$$

なる受信者識別情報r_X（σ_X，Ａ）を計算し、受信者識別情報r_X（σ_X，Ａ）を受信者xが使用する受信者装置xに送信するとともに、前記鍵管理者装置から受信した鍵配送データy_{Ai}と、整数ｒから、鍵配送情報

【数７９】

数79

$$z_{Ai} = y_{Ai}^{r} \ (\in G_A) \quad (1 \leq i \leq m)$$

を計算し、鍵配送情報z_{Ai}を、前記複数の受信者装置に同報送信する手順と、

【数８０】

数80

$$K_A = g_A^{rr'} \ (\in G_A)$$

に従って同報通信に用いる暗復号化鍵K_Aを計算する手順と、を実行させることを特徴とするプログラムが記憶された記憶媒体。

【請求項24】同報暗号通信を行う複数の送信者装置と、複数の受信者装置と、前記送信者装置が同報暗号通信に用いる暗復号化鍵の前記受信者装置への配送を支援する鍵管理者装置とを有する通信システムにおいて、前記受信者装置における処理をコンピュータに実行させるプログラムを記憶した記憶媒体であって、

当該プログラムは、コンピュータに、

送信者Aが使用する送信者装置Aから受信した受信者識別情報$r_X(\sigma_X, A)$および鍵配送情報z_{Ai}と、前記鍵管理者装置から配布された受信者秘密情報σ_X、$s_X(\sigma_X)$から、

【数81】

数81

$$K_A = \left(\prod_{i=1}^{k} z_{A\sigma_x(i)}\right)^{r_x(\sigma_x,A)s_x(\sigma_x)} \quad (\in G_A)$$

により、前記送信者装置Aが

【数82】

数82

$$K_A = g_A^{\pi'} \ (\in G_A)$$

によって生成し、同報通信に用いる暗復号化鍵K_Aを計算する手順と、を実行させることを特徴とするプログラムが記憶された記憶媒体。

【請求項25】同報暗号通信を行う通信システムにおいて、同報暗号通信に用いる暗復号化鍵を、送信者と受信者との間で共有するための鍵配送システムであって、

鍵管理者装置と、複数の送信者装置と、複数の受信者装置とを含み、

前記鍵管理者装置は、

鍵管理者秘密情報として、

【数83】

数83

$$c_i \in \mathbf{Z} \ (1 \le i \le m)$$

を作成し、送信者Aの送信者識別情報として、

【数84】

数84

$$t_A \in \mathbf{Z}$$

を作成し、受信者xの受信者秘密情報として、$\sigma_X \in S_{km}$と、

【数85】

数85

$$s_x(\sigma_x) \in \mathbf{Z}$$

（但し、集合

【数86】

数86

$$S_{km} = \{\sigma \mid 1\text{対}1\text{写像}\ \sigma : A = \{1,2,\cdots,k\} \to B = \{1,2,\cdots,m\}, 0 < k < m\}$$

に対して、σ、$\sigma' \in S_{km}$のとき

【数87】

数87

$$\sigma \sim \sigma' \iff \sigma(A) = \sigma'(A)$$

とし、このとき、～はS_{km}上の同値関係となり、

【数88】

数88

$$\tilde{S}_{km} = S_{km}/\sim$$

とする）とを作成し、受信者秘密情報σ_X、$s_X(\sigma_X)$を受信者xが使用する受信者装置xに配布する手段と、鍵管理者秘密情報e_i、送信者識別情報t_Aおよび受信者秘密情報$s_X(\sigma_X)$、σ_Xから、受信者識別データ

【数89】

数89

$$s_x(\sigma_x, A) = t_A s_x(\sigma_x) \sum_{i=1}^{k} e_{\sigma_x(i)}$$

を計算し、受信者識別データ$s_X(\sigma_X, A)$を送信者Aが使用する送信者装置Aに送信するとともに、送信者Aから受信したg_Aと、鍵管理者秘密情報e_iと、送信者識別情報t_Aから、鍵配送データ

【数90】

数90

$$y_{Ai} = g_A^{t_A c_i} \mod N_A \quad (1 \le i \le m)$$

を算出し、鍵配送データy_{Ai}を前記送信者装置Aに送信する手段と、を有し、

前記送信者装置Aは、

送信者Aの送信者秘密情報として、

【数91】

数91

$$P_A, Q_A : \text{素数}$$

$$L_A = \mathrm{lcm}(\mathrm{ord}_{P_A}(g_A), \mathrm{ord}_{Q_A}(g_A))$$

$$g_A \in \mathrm{Z}, 0 < g_A < N_A$$

を作成し、送信者Aの送信者公開情報として、

【数92】

数92

$$N_A (= P_A Q_A)$$

を作成し、送信者秘密情報g_Aを前記鍵管理者装置に送信する手段と、

整数r、r´を生成し、前記鍵管理者装置から受信した受信者識別データ$s_X(\sigma_X, A)$と、送信者秘密情報L_Aと、整数r´から

【数93】

数93

$$r_x(\sigma_x, A) s_x(\sigma_x, A) \equiv r' \pmod{L_A}$$

なる受信者識別情報$r_X(\sigma_X, A)$を計算し、受信者識別情報$r_X(\sigma_X, A)$を前記受信者装置xに送信するとともに、前記鍵管理者装置から受信した鍵配送データy_{Ai}と、整数rから、鍵配送情報

【数94】

数94

$$z_{Ai} = y_{Ai}{}^{r} \bmod N_A \quad (1 \le i \le m)$$

を計算し、鍵配送情報z_{Ai}を前記複数の受信者装置に同報送信する手段と、を有し、

前記受信者装置xは、

前記送信者装置Aから受信した受信者識別情報$r_X(\sigma_X, A)$および鍵配送情報z_{Ai}と、前記鍵管理者装置から配布された受信者秘密情報σ_X、$s_X(\sigma_X)$から、

【数95】

数95

$$K_A = \left(\prod_{i=1}^{k} z_{A\sigma_x(i)} \right)^{r_x(\sigma_x, A) a_x(\sigma_x)} \bmod N_A$$

により、前記送信者装置Aが

【数96】

数96

$$K_A = g_A{}^{r r'} \bmod N_A$$

によって生成し，同報通信に用いる暗復号化鍵K_Aを計算する手段と、を有することを特徴とする通信システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、同報暗号通信における復号に用いる鍵を限定された受信者に配送する鍵配送の技術に関するものである。

【0002】

【従来の技術】従来より、同報暗号通信の技術として、幾つかの方式が提案されている。

【0003】たとえば、文献「S.J.Kent:Security requirement and protocols for a broadcast scenario,IEEE Trans. Commun.,COM-29,6,pp.778-786(1981)」に記載のコピー鍵方式が知られている。

【0004】このコピー鍵方式は、同報暗号通信の基本的な方式であり、従来の1対1の暗号個別通信を単純に同報通信に拡張したものである。すなわち、この方式では、1種類の鍵のコピーを送信者と複数の正規の受信者に配送する。そして、送信者は配送されたコピー鍵を用いて情報を暗号化して送信し、正規の各受信者は配送されたコピー鍵を用いて暗号化された情報を復号化する。

【0005】また、このコピー鍵のように、送信者と受信者が共通に用いる鍵である共通鍵を、秘密裏に限定された受信者に配送する技術としては、文献「李、常盤他：多重化・多重分離法を用いた同報通信、1986年暗号と情報セキュリティシンポジウム」に記載の中国人の剰余定理を用いた情報系列の多重化・多重分離法による鍵配送方式や、文献「満保他：効率的な同報暗号通信方式、信学技法ISEC93-34（1993-10）」に記載の方式などが知られている。

【0006】中国人の剰余定理を用いて情報系列の多重化・多重分離法を行う方式は、次の処理を行うものである。

【0007】（1）鍵生成処理：受信者i（1≦i≦r）に対して、互いに素なs個の整数g_1，g_2，．．．，g_s（r≦s）を作成し、g_iを受信者iの秘密情報として、予め受信者iに配布する。

【0008】（2）暗号化処理：多重化すべきs個の情報系列をM_1，M_2，．．．，M_sとする。送信者は、多重化送信文Fを、

【0009】

【数97】

数97

$$F = \sum_{i=1}^{k} A_i G_i M_i \bmod G$$

【0010】により計算し、これを同報送信する。但し、G、G_i，A_iは、

【0011】

【数98】

数98

$$G = \prod_{i=1}^{k} g_i,$$
$$G_i = G/g_i,$$
$$A_i G_i \equiv 1 \pmod{g_i}$$

【0012】において、A_iが最小の整数となる関係にある。

【0013】（3）復号化処理：受信者iは、多重化送信文Fからg_iを用いて、

【0014】

【数99】

数99

$$M_i = F \bmod g_i$$

【0015】により、M_iを分離化する。

【0016】ここで、M_iは、受信者iに配送すべき共通鍵であってよい。したがって、この方式によれば、限定された受信者のみに秘密裏にコピー鍵を配送することができる。

【0017】次に、文献「満保他：効率的な同報暗号通信方式、信学技法ISEC93-34（1993-10）」に記載の方式は、次の処理を行うものである。

【0018】（1）鍵生成処理：信頼できるセンタは、次の情報を作成する。

【0019】秘密情報：

【0020】

【数100】

数100

$$P = 2p + 1, Q = 2q + 1 : \text{素数} \quad (p, q : \text{素数})$$
$$e_i \in \mathbb{Z},\ 0 < e_i < L \quad (1 \le i \le m)$$

【0021】公開情報：

【0022】

【数101】

数101

$$g \in \mathbb{Z},\ 0 < g < N$$
$$N = PQ$$
$$v_i = g^{e_i} \bmod N \quad (1 \le i \le m).$$

【0023】センタは、$\sigma \in S$に対して、

【0024】

【数102】

数102

$$s_\sigma \sum_{i=1}^{k} e_{\sigma(i)} \equiv 1 \pmod{L}$$

【0025】なるSσを計算し、受信者Uσの秘密情報として配布する。但し、集合S＝｛f｜1対1写像f：A＝｛1，2，．．．，k｝→B＝｛1，2，．．．，m｝、m＞k｝とする。

【0026】（2）鍵配送処理：送信者は整数rをランダムに選び、共通鍵

【0027】

【数103】

数103

$$K = g^r \bmod N$$

【0028】を限定された受信者との間で共有することを目的として、

【0029】

【数104】

数104

$$z_i = v_i{}^r \bmod N \qquad (1 \le i \le m)$$

【0030】を計算し、z_i（1≦i≦m）を同報送信する、受信者Uσは、

【0031】

【数105】

数105

$$K = \left(\prod_{i=1}^{k} z_{\sigma(i)} \right)^{s_\sigma} \bmod N$$

【００３２】にて、共通鍵Ｋを計算する。
【００３３】
【発明が解決しようとする課題】前述した中国人の剰余定理を用いた多重化方法を利用した鍵配送では、受信者一人一人用の共通鍵のデータをシリアルに並べて送信するので、受信者数に比例して同報通信するデータの長さが長くなる。このため、衛星放送サービスのように数百万人以上の受信者を対象とする通信には適していない。
【００３４】これに対して、文献「満保他：効率的な同報暗号通信方式、信学技法ISEC93-34（1993-10）」に記載の方式によれば、受信者数が大きい場合であっても共通鍵配送のためのデータを小さくできる。しかし、この方式では、任意の受信者集合に属する限定された受信者のみと鍵共有を行なうことができない。
【００３５】また、いずれの方式の場合も、送信者が複数存在する場合には、受信者は情報を受信する送信者毎に、それぞれ、前述した秘密情報を入手、管理しなければならない。
【００３６】そこで、本発明は、受信者が唯一の秘密情報によって、複数の送信者からの個々の共通鍵の配送を受けることのできる鍵配送システムを提供することを課題とする。また、このような鍵配送システムにおいて、任意の送信者と任意の受信者集合に属する受信者のみとのデータ暗復号のための共通鍵の共有を可能とすること、および、受信者数が大きい場合に、これに伴い共通鍵配送のための同報通信データを長くする必要がない共通鍵配送を実現することを課題とする。
【００３７】
【課題を解決するための手段】前記課題達成のために、本発明は、複数の送信者と 複数の受信者とが存在する通信システムにおいて、前記送信者が行う同報暗号通信の暗復号化鍵を、前記送信者と前記受信者との間で共有するための鍵配送方法であって、鍵管理者を設け、当該鍵管理者において、前記送信者と前記受信者との間で鍵を共有するために用いる、前記複数の送信者について共通の第１鍵情報を作成して所定の受信者に配布するとともに、前記送信者と前記受信者との間で鍵を共有するするために用いる第２鍵情報を作成して前記送信者に配布し、前記送信者は、前記受信者が前記第１鍵情報を用いて当該送信者が同報通信に用いる暗復号化鍵を算出するための第３鍵情報を、前記鍵管理者から配布された第２鍵情報を用いて生成して、当該送信者と鍵を共有する前記受信者に送信し、前記受信者は、前記鍵管理者から配布された第１鍵情報と前記送信者から配布された第３鍵情報とを用いて、第３鍵情報を配布した前記送信者が同報通信に用いる暗復号化鍵を入手することを特徴とする。
【００３８】本鍵配送方法によれば、各受信者は、秘密情報として鍵管理者から配布された第１鍵情報のみを所持すればよく、新たな送信者の暗復号化鍵を入手する場合にも、新たな秘密情報の配布を受ける必要がない。
【００３９】より詳細には、本発明は、前記課題達成のために、たとえば、複数の送信者と、複数の受信者と、鍵管理者とが存在する通信システムを用い、前記送信者が行う同報暗号通信の暗復号化鍵を、前記受信者に配送する鍵配送方法であって、鍵管理者において、鍵管理者秘密情報として、
【００４０】
【数１０６】

数106

$$e_i \in \mathbb{Z}, \quad (1 \le i \le m)$$

【００４１】を作成し、送信者Ａの送信者識別情報として、
【００４２】
【数１０７】

数107

$$t_A \in \mathbb{Z}$$

【００４３】を作成し、受信者ｘの受信者秘密情報として、$\sigma_x \in S_{km}$と、
【００４４】
【数１０８】

数108

$$s_x(\sigma_x) \in \mathbb{Z}$$

【００４５】（但し、集合
【００４６】
【数１０９】

数109

$$S_{km} = \{\sigma \mid 1\text{対}1\text{写像}\ \sigma : A = \{1,2,\cdots,k\} \to B = \{1,2,\cdots,m\}, 0 < k < m\}$$

【００４７】に対して、σ、σ' $\in S_{km}$のとき
【００４８】
【数１１０】

数110

$$\sigma \sim \sigma' \quad \overset{def}{\Longleftrightarrow} \quad \sigma(A) = \sigma'(A)$$

【0049】とし、このとき、～はS_{km}上の同値関係となり、

【0050】

【数111】

数111

$$\tilde{S}_{km} = S_{km} / \sim$$

【0051】とする）とを作成し、受信者秘密情報σ_X、s_X（σ_X）を受信者xに配布するステップと、送信者Aにおいて、

【0052】

【数112】

数112

- $g_A \in G_A$
- $L_A = \mathrm{ord}_{G_A}(g_A)$

【0053】（但し、

【0054】

【数113】

数113

$$\mathrm{ord}_{G_A}(g)$$

【0055】は、

【0056】

【数114】

数114

$$g^a = 1 \ (\in G_A)$$

【0057】なる最小の正整数aを表す）なる送信者秘密情報g_A、L_Aおよび有限アーベル群G_Aを作成し、送信者秘密情報g_Aを鍵管理者に送信するステップと、鍵管理者において、鍵管理者秘密情報e_i、送信者識別情報t_Aおよび受信者秘密情報s_X（σ_X）、σ_Xから、受信者識別データ

【0058】

【数115】

数115

$$s_x(\sigma_x, A) = t_A s_x(\sigma_x) \sum_{i=1}^{k} e_{\sigma_x(i)}$$

【0059】を計算し、受信者識別データs_X（σ_X，A）を送信者Aに送信し、送信者Aから受信したg_Aと、鍵管理者秘密情報e_iと、送信者識別情報t_Aから、鍵配送データ

【0060】

【数116】

数116

$$y_{Ai} = g_A^{t_A e_i} \ (\in G_A) \quad (1 \le i \le m)$$

【0061】を算出し、鍵配送データy_{Ai}を送信者Aに送信するステップと、送信者Aにおいて、整数r、r⁻を生成し、鍵管理者から受信した受信者識別データs_X（σ_X，A）と、送信者秘密情報L_Aと、整数r⁻から

【0062】

【数117】

数117

$$r_x(\sigma_x, A) s_x(\sigma_x, A) \equiv r' \pmod{L_A}$$

【0063】なる受信者識別情報r_X（σ_X，A）を計算し、受信者識別情報r_X（σ_X，A）を受信者xに送信し、鍵管理者から受信した鍵配送データy_{Ai}と、整数rから、鍵配送情報

【0064】

【数118】

数118

$$z_{Ai} = y_{Ai}^{r} \ (\in G_A) \quad (1 \le i \le m)$$

【0065】を計算し、鍵配送情報z_{Ai}を、各受信者に同報送信するステップと、受信者xにおいて、送信者Aから受信した受信者識別情報r_X（σ_X，A）および鍵配送情報z_{Ai}と、鍵管理者から配布された受信者秘密情報σ_X、s_X（σ_X）から、

【0066】

【数119】

数119

$$K_A = \left(\prod_{i=1}^{k} z_{A\sigma_x(i)} \right)^{r_x(\sigma_x, A) s_x(\sigma_x)} \ (\in G_A)$$

【0067】により、送信者Aが

【0068】

【数120】

数120

$$K_A = g_A^{rr'} \ (\in G_A)$$

【0069】によって生成し、同報通信に用いる暗復号化鍵K_Aを計算するステップと、を有することを特徴とする。

【0070】この鍵配送方法によれば、受信者は送信者毎に異なる秘密鍵を持つ必要がない他、同報暗号通信において、受信者数が大きい場合であっても、これに伴い

鍵配送情報の長さを長くする必要がない。また、本鍵配送方法においては、鍵管理者のみが秘密裏に所持する送信者識別情報によって、受信者秘密情報は送信者に対して秘密化され、受信者に対して送信者秘密情報はより強固に秘密化されるので、不正に対する安全性が向上する。

【００７１】

【発明の実施の形態】以下、本発明に係る鍵配送システムの実施形態について説明する。

【００７２】まず、本発明の第１実施形態について説明する。

【００７３】図１に、本発明の第１実施形態に係る鍵配送システムの構成を示す。

【００７４】図示するように、本システムは、相互に通信回線４００で接続された鍵管理者側装置１００、送信者側装置２００、受信者側装置３００から構成される。鍵管理者側装置１００は、システムに唯一の鍵管理者組織が使用する装置であり、送信者装置２００、受信者側装置３００はシステム中に複数存在する。

【００７５】図２に、鍵管理者側装置１００の構成を示す。

【００７６】図示するように、鍵管理者側装置１００は、乱数生成器１０１、素数生成器１０２、べき乗算器１０３、剰余演算器１０４、演算装置１０５、メモリ１０６、通信装置１０７から構成される。また、鍵管理者側装置１００には、オフラインで受信者に配送する受信者側携帯装置３０６が接続される。

【００７７】図３に、送信者側装置２００の構成を示す。

【００７８】図示するように、送信者側装置２００は、乱数生成器２０１、素数生成器２０２、べき乗算器２０３、剰余演算器２０４、演算装置２０５、メモリ２０６、通信装置２０７、暗復号化装置２０８、認証装置２０９、課金装置２１０から構成される。

【００７９】図４に、受信者側装置３００の構成を示す。

【００８０】図示するように、受信者側装置３００は、べき乗算器３０１、剰余演算器３０２、演算装置３０３、メモリ３０４、通信装置３０５、鍵管理者からオフラインで配送された受信者側携帯装置３０６、暗復号化装置３０７、認証装置３０８から構成される。

【００８１】以下、本システムが行う準備処理、鍵配送処理、そして暗復号化処理の３つの処理について説明する。

【００８２】では、まず、準備処理について説明する。

【００８３】（１）準備処理

❶送信者Ａは、送信者側装置２００内の乱数生成器２０１、素数生成器２０２、べき乗算器２０３、剰余演算器２０４、および演算装置２０５を用いて、次の情報を作成し、そのうち、公開情報のみを公開する。

【００８４】秘密情報：

【００８５】

【数１２１】

数121

$$P_A, Q_A : \text{素数}$$

$$L_A = \mathrm{lcm}(\mathrm{ord}_{P_A}(g_A), \mathrm{ord}_{Q_A}(g_A))$$

$$g_A \in \mathbf{Z}, \quad 0 < g_A < N_A$$

【００８６】公開情報：

【００８７】

【数１２２】

数122

$$N_A (= P_A Q_A)$$

【００８８】秘密情報はメモリ２０６に格納する。また、秘密情報g_A、L_Aを通信装置２０７を用いて鍵管理者に送信する。

【００８９】❷信頼できる鍵管理者は、鍵管理者側装置１００内の演算装置１０５を用いて、次の情報を作成する。

【００９０】鍵管理者秘密情報：

【００９１】

【数１２３】

数123

$$e_i \in \mathbf{Z} \ (1 \leq i \leq m)$$

【００９２】送信者Ａの送信者識別情報：

【００９３】

【数１２４】

数124

$$t_A \in \mathbf{Z}, \quad 0 < t_A < L_A$$

【００９４】受信者ｘの受信者秘密情報：

【００９５】

【数１２５】

数125

$$s_x(\sigma_x) \in \mathbf{Z}, \quad 0 < t_A < L_A$$

【００９６】これらは、σ_Xとともに全てメモリ１０６に格納する。

【００９７】ただし、集合

【００９８】

【数１２６】

数126

$$S_{km} = \{\sigma \mid 1\text{対}1\text{写像}\ \sigma : A = \{1,2,\cdots,k\} \to B = \{1,2,\cdots,m\}, 0 < k < m\}$$

【００９９】に対して、σ、σ´∈S_{km}のとき、
【０１００】
【数１２７】

数127

$$\sigma \sim \sigma' \quad \overset{\text{def}}{\Longleftrightarrow} \quad \sigma(A) = \sigma'(A)$$

【０１０１】とする。このとき、～はS_{km}上の同値関係となり、
【０１０２】
【数１２８】

数128

$$\tilde{S}_{km} = S_{km} / \sim$$

【０１０３】とする。
【０１０４】また、鍵管理者は、メモリ１０６から受信者秘密情報s_X（σ_X）を取り出し、σ_Xとともに受信者側携帯装置３０６に格納し、これを受信者xにオフラインで配布する。もちろん、他の方法によって受信者に配布するようにしてもよい。
【０１０５】次に、鍵配送処理について説明する。
【０１０６】（２）鍵配送処理
本鍵配送処理における、鍵管理者、送信者、および受信者間の情報の流れを図５に示す。
【０１０７】㋐鍵管理者は、鍵管理者側装置１００内の剰余演算器１０４、演算装置１０５を用いて、送信者Aから受信したL_Aと、鍵管理者秘密情報e_iと、受信者秘密情報σ_X、s_X（σ_X）と、送信者識別情報t_Aから、
【０１０８】
【数１２９】

数129

$$s_x(\sigma_x, A) = t_A s_x(\sigma_x) \sum_{i=1}^{k} e_{\sigma_x(i)} \mod L_A$$

【０１０９】なる受信者xの受信者識別データs_X（σ_X，A）を計算し、通信装置１０７を用いて送信者Aに送信する。
【０１１０】また、鍵管理者は、鍵管理者側装置１００内のべき乗算器１０３、剰余演算器１０４、演算装置１０５を用いて、送信者Aから受信したg_Aと、送信者Aの送信者公開情報N_Aと、鍵管理者秘密情報e_iから、
【０１１１】
【数１３０】

数130

$$y_{Ai} = g_A^{i_A e_i} \mod N_A \quad (1 \le i \le m)$$

【０１１２】なる送信者Aの送信者鍵配送データy_{Ai}を計算し、通信装置１０７を用いて送信者Aに送信する。
【０１１３】㋑送信者Aは、送信者側装置２００内の乱数生成器２０１により、乱数r、r´を作成しメモリ２０６に格納する。さらに、べき乗算器２０３、剰余演算器２０４、演算装置２０５を用いて、この乱数r、r'と、自身の秘密情報g_Aと、自身の公開情報N_Aから、
【０１１４】
【数１３１】

数131

$$K_A = g_A^{rr'} \mod N_A$$

【０１１５】なるデータ暗号化鍵K_Aを計算してメモリ２０６に格納し、受信者xとの間で鍵K_Aを共有することを目的として、剰余演算器２０４、演算装置２０５を用いて、自身の秘密情報L_Aと、乱数r´と、鍵管理者から受信した受信者xの受信者識別データs_X（σ_X，A）から、
【０１１６】
【数１３２】

数132

$$r_x(\sigma_x, A) s_x(\sigma_x, A) \equiv r' \pmod{L_A}$$

【０１１７】なる受信者xの受信者識別情報r_X（σ_X，A）を計算し、通信装置２０７を用いて受信者xに送信する。
【０１１８】また、送信者Aは、送信者側装置２００内のべき乗算器２０３、剰余演算器２０４、演算装置２０５を用いて、自身の公開情報N_Aと、乱数rと、鍵管理者から受信した送信者鍵配送データy_{Ai}から、
【０１１９】
【数１３３】

数133

$$z_{At} = y_{Ai}^{r} \bmod N_A \quad (1 \le i \le m)$$

【０１２０】なる受信者鍵配送データz_{Ai}を計算し、通信装置２０７を用いて受信者に同報送信する。
【０１２１】ここで、以上の処理において、r_X（σ_X，A）、z_{Ai}を作成する処理の一部を、鍵管理者が行う理由の一つは、送信者Aに対して、受信者xの受信者秘密情報σ_X、s_X（σ_X）、送信者識別番号t_Aを秘密にすることにより、送信者Aの不正を防止するためである。
【０１２２】㋒受信者xは、送信者Aから受信した鍵配送データz_{Ai}および受信者識別情報r_X（σ_X，A）、鍵管理者から配送された受信者秘密情報σ_X、s_X（σ_X）、公開された送信者公開情報N_Aから、

【0123】
【数134】
数134

$$K_A = \left(\prod_{i=1}^{k} z_{A\sigma_x(i)} \right)^{r_x(\sigma_x, A) s_x(\sigma_x)} \mod N_A$$

【0124】により、データ暗号化鍵K_Aを計算し、メモリ304に格納する。
【0125】以上の処理で、送信者Aと受信者xは鍵K_Aを共有できる。他の任意の送信者と受信者についても同様にして鍵を共有できる。また、この際、送信者Aが同報送信する受信者鍵配送データz_{Ai}は、各受信者について共通である。
【0126】また、以上の処理において、受信者xが送信者Aより受けとる鍵配送データz_{Ai}および受信者識別情報$r_X(\sigma_X, A)$は、受信者に対して秘密化されている送信者Aの送信者識別番号t_Aが作用したものとなっている。したがって、以上の送信者識別番号t_Aを用いる構成により、受信者xが送信者Aより受けとった鍵配送データz_{Ai}、受信者識別情報$r_X(\sigma_X, A)$、他の送信者Bの公開情報N_B、他の送信者Bが同報通信した鍵配送データz_{Bi}より、他の送信者Bのデータ暗号化鍵K_Bを割り出すことを、きわめて困難とすることができる。
【0127】以下、暗復号化処理について説明する。
【0128】（3）暗復号化処理
①送信者Aは、送信者側装置200内の暗復号化装置208を用いて、鍵配送処理で作成した共通鍵K_Aにより、データPを暗号化する。そして、暗号文C＝E（K_A：P）を通信装置207を用いて受信者xに送信する。
【0129】②受信者xは、受信者側装置300内の通信装置305を用いて暗号文Cを受信し、暗復号化装置307を用いてメモリ304に格納していた共通鍵K_Aにより暗号文Cを復号化し、データを得る。
【0130】以上、本発明の第1実施形態について説明した。
【0131】従来の技術では、新規に送信者がシステムに参入する際、受信者秘密情報σ_X、$s_X(\sigma_X)$を、送信者自身が作成し受信者にオフラインで配布する必要があった。これに対し、第1実施形態に係る鍵配送システムによれば、新規参入の送信者Aは、送信者秘密情報P_A、Q_A、L_A、g_Aと、送信者公開情報N_Aを作成するだけでよい。また、受信者が持つ受信者秘密情報は、全ての送信者に対して唯一であり、新たな送信者からデータを受信したい場合に、新たな受信者秘密情報を入手する必要がない。
【0132】また、受信者識別情報$r_X(\sigma_X, A)$によって、任意の受信者集合に属する受信者のみとのデータ暗復号のための共通鍵の共有を可能とすることができる。また、受信者数が大きい場合であっても、共通鍵配送のために同報通信する鍵配送データz_{Ai}を、これに伴い長くする必要がない。
【0133】なお、以上の処理において、あらかじめ、送信者Aが送信者秘密情報L_Aを鍵管理者に送信しておき、準備処理の段階で、鍵管理者は、送信者Aから受信した送信者秘密鍵L_Aから
【0134】
【数135】
数135

$$e_i \in \mathbb{Z}, \quad 0 < e_i < L_A, \quad (1 \le i \le m)$$

$$t_A \in \mathbb{Z}, \quad 0 < t_A < L_A$$

$$s_x(\sigma_x) \in \mathbb{Z}, \quad 0 < s_x(\sigma_x) < L_A$$

【0135】となる鍵管理者秘密情報e_i、送信者識別情報t_A、受信者秘密情報$s_X(\sigma_X)$を作成し、鍵配送処理の段階で、鍵管理者は、送信者秘密情報L_A、鍵管理者秘密情報e_i、送信者識別情報t_A、受信者秘密情報$s_X(\sigma_X)$から、
【0136】
【数136】
数136

$$s_x(\sigma_x, A) = t_A s_x(\sigma_x) \sum_{i=1}^{k} e_{\sigma_x(i)} \mod L_A$$

【0137】によって、受信者識別データ$s_X(\sigma_X, A)$を計算するようにしてもよい。
【0138】次に、本発明の第2実施形態について説明する。
【0139】本発明の第2実施形態は、上記の第1実施形態における受信者側携帯装置306に、図6に示すように、べき乗算器3036、剰余演算器3063、演算装置3061、メモリ3062を備えるようにしたものである。そして、上記の第1実施形態の受信者側装置300におけるデータ暗号化鍵K_Aの計算処理の一部を、受信者側携帯装置306で実施するようにしたものである。
【0140】すなわち、第2実施形態では、（1）準備処理の段階で、鍵管理者はσ_Xと受信者秘密情報$s_X(\sigma_X)$とを、受信者携帯装置306（ICカード等）に格納して、受信者xに配布する。
【0141】そして、（2）鍵配送処理において、受信者xは、受信者側装置300内のメモリに格納されている鍵配送データz_{Ai}を受信者携帯装置306に出力する。次に、受信者携帯装置306内で、べき乗算器3064、剰余演算器3063を用いて、受信者秘密情報σ

$_X$、$s_X(\sigma_X)$、鍵配送データz_{Ai}および送信者公開情報N_Aから、

【0142】

【数137】

数137

$$\xi_x(\sigma_x, A) = \left(\prod_{i=1}^{k} z_{A\sigma_x(i)}\right)^{s_x(\sigma_x)} \bmod N_A$$

【0143】を計算し、この計算結果$\xi_X(\sigma_X, A)$を受信者側装置300に出力する。

【0144】次に、受信者側装置300内のべき乗算器301、剰余演算器302、演算装置303を用いて、受信者側装置300に出力された$\xi_X(\sigma_X, A)$と、メモリ304に格納している受信者識別鍵$r_X(\sigma_X, A)$および送信者公開情報N_Aから、

【0145】

【数138】

数138

$$K_A = \xi_x(\sigma_x, A)^{r_x(\sigma_x, A)} \bmod N_A$$

【0146】により、データ暗号化鍵K_Aを計算し、メモリ304に格納する。

【0147】このように受信者秘密情報σ_X、$s_X(\sigma_X)$が受信者側携帯装置306外部に出力しないようにすることにより、これが電子的複写などにより盗難されることを防ぐことができる。

【0148】以上、本発明の第2実施形態について説明した。

【0149】次に、本発明の第3実施形態について説明する。

【0150】本発明の第3実施形態は、上記の第1実施形態において、

【0151】

【数139】

数139

$$K_A = g_A^{rr'} \bmod N_A$$

【0152】のrの値を短時間毎に、周期毎に変更し、変更後のrを用いたz_{Ai}を周期的に同報通信することにより、送信者側装置200および受信者側装置300で計算するデータ暗復号化鍵K_Aの更新を行うものである。

【0153】また、r´の値を送信データ固有の値とすることで、送信者が同報送信するデータの識別を行うようにしたものである。すなわち、受信者xがある同報データもしくは同報データの集合を復号するために、ある送信者から得た識別鍵$r_X(\sigma_X, A)$はその同報データ固有のものであり、別の同報データもしくは同報データの集合を取得するためには、その送信者から別の同報データもしくは同報データの集合用の別の$r_X(\sigma_X, A)$を得る必要がある。

【0154】以上、本発明の第3実施形態について説明した。

【0155】次に、本発明の第4実施形態について説明する。

【0156】本発明の第4実施形態は、上記の第1実施形態において、特定の受信者の認証を行い、送信者が鍵K_Aを用いて暗号化し送信した有償のデータPに対する、鍵K_Aを共有する受信者への課金を行うものである。

【0157】すなわち、第4実施形態では、さらに、以下の処理を行う。

【0158】（1）準備処理

① 鍵管理者は、鍵管理者側装置100内の演算装置105を用いて、予め受信者xの番号UID_Xを作成し、これを受信者秘密情報$s_X(\sigma_X)$と一緒に受信者携帯装置306内のメモリ3061に格納して配布する。また、UID_Xを、$s_X(\sigma_X)$と対応させて、鍵管理者側装置100内のメモリ106に格納しておく。

【0159】② 送信者Aは、送信者側装置200内の演算装置205を用いて、自身の番号BID_Aを作成し、メモリ206に格納しておく。また、BID_Aを通信装置207を用いて鍵管理者に送信する。

【0160】③ 鍵管理者は、鍵管理者側装置100内の通信装置107によって送信者Aの番号BID_Aを受信し、メモリ106に送信者識別情報t_Aと対応させて格納する。

【0161】④ 受信者xは、受信者側装置300内の認証装置308を用いて、受信者秘密情報$s_X(\sigma_X)$から認証用の情報を作成し、送信者Aに送信する。

【0162】⑤ 送信者Aは、該認証用の情報を、送信者側装置200内の認証装置209によって確認する。

【0163】この認証の方法は、受信者が$s_X(\sigma_X)$を知らない限り、認証が成立しない認証方法であれば、従来知られている各種認証方式を用いてかまわない（ただし、このとき、送信者は受信者秘密鍵$s_X(\sigma_X)$自体は知ることができないようにする必要がある）。

【0164】たとえば、RSA（文献「R. L, Rivest, A. Shamir, L. Adelman. :A methodfor obtaining digital signatures and publickey cryptosystems, Commun. of the ACM, Vol. 21, No.2,pp.120-126, 1987.」に掲載）による署名を用いた方法によって、受信者xの認証を、以下の処理によって行えばよい。

【0165】1:鍵管理者は、受信者xに対して、

【0166】

【数140】

数140

$$s'_x y_x \equiv 1 \pmod{\mathrm{lcm}(p_x - 1, q_x - 1)}$$
$$n_x = p_x q_x \quad (p_x, q_x : \text{素数})$$

【0167】なる（y_X，n_X）を予め送信者に配布する。ただし、公開された関数πに対して、$s'_X = \pi(s_X(\sigma_X))$とする。

【0168】2:受信者xは、受信者側装置300内の認証装置308を用いて、同報送信データであるWのハッシュ値を、公開情報である一方向性ハッシュ関数hにより計算し（0＜h（W）＜n_X）、h（W）に対する署名を秘密鍵s'_Xを用いて、

【0169】

【数141】

数141

$$\mathrm{sgn}_x(h(W)) = h(W)^{s'_x} \bmod n_x$$

【0170】にて作成し、データの送信要求とともに通信装置305を用いて送信者Aに送信する。

【0171】3:送信者Aは、認証装置209を用いて、

【0172】

【数142】

数142

$$\mathrm{sgn}_x(h(W))^{y_x} \equiv h(W) \pmod{n_x}$$

【0173】が成立することを確認する。

【0174】④さて、認証を行った後に、送信者Aは、送信者側装置200内の通信装置207を用いて、自身の番号BID_Aと受信者xの番号UID_Xを鍵管理者に送信する。

【0175】⑦鍵管理者は、鍵管理者側装置100内の演算装置105を用いて、受信した送信者番号BID_Aと受信者番号UID_Xに対応した、送信者識別鍵t_Aと受信者秘密情報$s_X(\sigma_X)$から、

【0176】

【数143】

数143

$$s_x(\sigma_x, A) = t_A s_x(\sigma_x) \sum_{i=1}^{k} e_{\sigma_x(i)} \bmod L_A$$

【0177】となる受信者識別データ$s_X(\sigma_X, A)$を計算し、送信者Aに送信する。

【0178】⑧送信者Aは、送信者側装置200内の剰余演算器204、演算装置205を用いて、鍵管理者から受信した受信者識別データ$s_X(\sigma_X, A)$から、

【0179】

【数144】

数144

$$r_x(\sigma_x, A) s_x(\sigma_x, A) \equiv r' \pmod{L_A}$$

【0180】となる受信者識別情報$r_X(\sigma_X, A)$を計算し、通信装置207により受信者xに送信する。その際、共通鍵K_Aによって、暗号化して配信するデータ（受信者が送信要求したデータ）が有償の場合、送信者Aは、課金装置210を用いて受信者xに対して課金する。

【0181】以上、本発明の第4実施形態について説明した。

【0182】次に、本発明の第5実施形態について説明する。

【0183】本発明の第5実施形態は、従来の技術の欄で述べたコピー鍵方式を、図1に示した複数の送信者と複数の受信者と鍵管理者が存在するシステムに拡張したものである。

【0184】図7に、本発明の第5実施形態に係る鍵管理者側装置100の構成を示す。図示するように、鍵管理者側装置100は、乱数生成器111、演算装置112、メモリ113、通信装置114から構成される。また、図8に、本発明の第5実施形態に係る送信者側装置200の構成を示す。図示するように、送信者側装置200は、乱数生成器211、演算装置212、暗復号化装置213、メモリ214、通信装置215から構成される。また、図9に、本発明の第5実施形態に係る受信者側装置300の構成を示す。図示するように、受信者側装置300は、演算装置311、暗復号化装置312、メモリ313、通信装置314から構成される。

【0185】本実施形態では、まず、準備処理として、以下の処理を行う。

【0186】（1）準備処理

①鍵管理者は、鍵管理者側装置100内の乱数生成器111を用いて、秘密情報K0を生成しメモリ113に格納する。また、送信者と受信者に配布する。

【0187】②送信者Aは、送信者側装置200内の乱数生成器211を用いて送信者識別情報BID_Aを生成し、通信装置114により受信者に送信する。

【0188】その後、鍵配送処理として、以下の処理を行う。

【0189】（2）鍵配送処理

③送信者Aは、送信者側装置200内の演算装置205を用いて、鍵管理者から配布された秘密鍵情報K0と送信者識別情報BID_Aから、適当な一方向性関数Fにより、共通鍵$K_A = F(K0, BID_A)$を計算する。

【0190】④受信者は、受信者側装置300内の演算装置312を用いて、鍵管理者から配布された秘密情報K0と送信者から受信した送信者識別情報BID_Aから、一方向性関数Fにより、共通鍵$K_A = F(K0,$

BID_A）を計算する。

【0191】③送信者Aは、送信者側装置200内の乱数生成器211を用いて適当な整数rを作成し、通信装置215により受信者に送信する。また、演算装置212を用いて、整数rと共通鍵K_A^-から、適当な関数F^-によりデータ暗復号化鍵$DK=F^-(r, K_A^-)$を計算し、メモリ214に格納する。

【0192】④受信者は、受信者側装置300内の演算装置312を用いて、送信者Aから受信した整数rと、共通鍵K_A^-から、関数F^-により、データ暗復号化鍵$DK=F^-(r, K_A^-)$を計算して、メモリ314に格納する。

【0193】上記の鍵配送処理により、データ暗復号化鍵DKの配送が行われた後、暗復号化処理は、以下の要領で行う。

【0194】（3）暗復号化処理

①送信者Aは、データ暗復号化鍵DKを用いて、送信者側装置200内の暗復号化装置203により配信データPを暗号化し、通信装置205により受信者に送信する。

【0195】②受信者は、受信者側装置300内の通信装置305により暗号化された配信データPを受信し、データ暗復号化鍵DKを用いて暗復号化装置303により復号化する。

【0196】以上説明した本発明の第5実施形態によっても、受信者は、単一の秘密情報で、複数の送信者と、各送信者個々の共通鍵を共有することができる。

【0197】次に、本発明の第6実施形態について説明する。

【0198】本発明の第6実施形態は、送信者と受信者が、受信者の個別の鍵を使った暗号通信により、共通鍵を共有するものである。

【0199】本実施形態に係る全体のシステム、鍵管理者側装置100、送信者側装置200、受信者側装置300の構成は、上述した本発明の第5実施形態のものと同様である。

【0200】さて、本実施形態では、準備処理において、以下の処理を行う。

【0201】（1）準備処理

①鍵管理者は、鍵管理者側装置100内の乱数生成器111を用いて受信者xの秘密情報s_Xを作成し、受信者に配布する。さらに、乱数生成器111を用いて送信者Aの番号BID_Aを作成し、送信者Aおよび受信者xに配布する。

【0202】②送信者Aは、送信者側装置200内の乱数生成器211を用いて共通鍵K_Aを作成する。

【0203】その後、鍵配送処理において、以下の処理を行う。

【0204】（2）鍵配送処理

①鍵管理者は、鍵管理者側装置100内の演算装置112を用いて、送信者Aの番号BID_Aと受信者秘密情報s_Xから、適当な一方向性関数Fにより$K_{AX}=F(s_X, K_A)$なる、受信者xおよび送信者A間でのセッション鍵K_{AX}を計算し、メモリ113に格納する。

【0205】②受信者xは、受信者側装置300内の演算装置312を用いて、送信者Aの番号BID_Aと自身の秘密情報s_Xから、一方向性関数Fにより$K_{AX}=F(s_X, BID_A)$を計算し、メモリ313に格納する。

【0206】③送信者Aは、送信者側装置200内の暗復号化装置213を用いて、セッション鍵K_{AX}により共通鍵K_Aを暗号化し、その結果、得られた鍵配送データK_{CX}を、通信装置215により受信者に送信する。さらに、乱数生成器211を用いて、適当な整数rを作成し、通信装置215により受信者に送信するとともに、演算装置212を用いて、整数rと共通鍵K_Aから、適当な関数F^-によりデータ暗復号化鍵$DK=F^-(r, K_A)$を計算し、メモリ214に格納する。

【0207】④受信者xは、受信者側装置300内の暗復号化装置303を用いて、送信者Aから受信した鍵配送データK_{CX}をセッション鍵K_{AX}により復号化する。そして、演算装置302を用いて、復号化した共通鍵K_Aと受信した整数rから、関数F^-により、データ暗復号化鍵$DK=F^-(r, K_A)$を計算し、メモリ303に格納する。

【0208】上記の鍵配送処理により、データ暗復号化鍵DKの配送が行われた後、暗復号化処理は、以下の要領で行う。

【0209】①送信者Aは、送信者側装置200内の暗復号化装置203を用いて、データ暗復号化鍵DKにより配信データPを暗号化し、通信装置205により受信者xに送信する。

【0210】②受信者xは、受信者側装置300内の通信装置305により暗号化された配信データPを受信する。そして、暗復号化装置303を用いて、受信した配信データPをデータ暗復号化鍵DKにより復号する。

【0211】なお、送信者Aは、共通鍵K_Aの値を周期的に変更することで、データ暗復号化鍵DKの値を周期的に変更することができる。

【0212】以上説明した本発明の第6実施形態によっても、受信者は、単一の秘密情報で、複数の送信者と、各送信者個々の共通鍵を共有することができる。

【0213】次に、本発明の第7実施形態について説明する。

【0214】本発明の第7実施形態は、上記の第6実施形態と同様、送信者と受信者が、受信者の個別の鍵を使った暗号通信により、共通の鍵を共有するものである。

【0215】本実施形態に係る全体のシステム、鍵管理者側装置100、送信者側装置200、受信者側装置300の構成は、上述した本発明の第5実施形態のものと同様である。

【0216】本発明の第7実施形態では、準備処理において、以下の処理を行う。

【0217】（1）準備処理

① 鍵管理者は、鍵管理者側装置100内の乱数生成器111、演算装置112を用いて、適当な公開鍵暗号Eに従った受信者xの秘密鍵s_Xおよび公開鍵p_Xを作成し、s_Xを受信者に配布する。さらに、乱数生成器111により送信者Aの番号BID_Aを作成し、送信者Aおよび受信者xに配布または送信する。

【0218】② 送信者Aは、送信者側装置200内の乱数生成器201を用いて共通鍵K_Aを作成し、メモリ114に格納する。

【0219】その後、鍵配送処理として、以下の処理を行う。

【0220】（2）鍵配送処理

③ 送信者Aは、送信者側装置200内の暗復号化装置213を用いて、前記適当な公開鍵暗号Eにより、受信者公開鍵p_Xと共通鍵K_Aから鍵配送データ$K_{CX}=E(p_X, K_A)$を計算する。その後、通信装置215によりK_{CX}を受信者xに送信する。

【0221】④ 受信者xは、受信者側装置300内の暗復号化装置313を用いて、送信者Aから受信した鍵配送データK_{CX}を自身の秘密鍵s_Xにより復号化し、復号化した共通鍵K_Aをメモリ314に格納する。

【0222】⑤ 送信者Aは、送信者側装置200内の乱数生成器201を用いて適当な整数rを生成し、通信装置215により受信者xに送信する。また、演算装置212を用いて、整数rと共通鍵K_Aから、適当な関数Fによりデータ暗復号化鍵$DK=F(r, K_A)$を計算し、メモリ204に格納する。

【0223】⑥ 受信者xは、受信者側装置300内の演算装置312を用いて、共通鍵KAと送信者から受信した整数rから、関数Fによりデータ暗復号化鍵$DK=(r, K_A)$を計算し、メモリ314に格納する。

【0224】上記の鍵配送処理により、データ暗復号化鍵DKの配送が行われた後、暗復号化処理は、以下の要領で行う。

【0225】（3）暗復号化処理

⑦ 送信者Aは、送信者側装置200内の暗復号化装置203を用いて、データ暗復号化鍵DKにより配信データPを暗号化し、通信装置205により受信者xに送信する。

【0226】⑧ 受信者xは、受信者側装置300内の通信装置305を用いて、暗号化された配信データPを受信する。そして、暗復号化装置303を用いて、受信した配信データPをデータ暗復号化鍵DKにより復号化する。

【0227】⑨ 送信者Aは、共通鍵KAの値を周期的に変更することによりデータ暗復号化鍵DKを変更する。

【0228】以上説明した本発明の第7実施形態によっても、受信者は、単一の秘密情報で、複数の送信者と、各送信者個々の共通鍵を共有することができる。

【0229】次に、本発明の第8実施形態について説明する。

【0230】本発明の第8実施形態は、上述した本発明の第6および第7実施形態において、送信者による鍵配送データK_{CX}の受信者への送信を、以下のように修正したものである。

【0231】すなわち、第8実施形態では、送信者Aは、受信者全体の集合をいくつかの部分集合にわける。次に、鍵配送データK_{Ci}（$1 \leqq i \leqq n$　ただし、nは受信者数）を受信者に送信する際、前記受信者の部分集合毎に通信チャンネルを割り当て、送信者側装置200内の通信装置215により受信者に送信する。

【0232】一方、任意の受信者xは、自身の属する部分集合に割り当てられた通信チャンネルを通じて、受信者側装置300内の通信装置305により、鍵配送データK_{CX}を受信する。

【0233】以上、本発明の第8実施形態について説明した。

【0234】次に、本発明の第9実施形態について説明する。

【0235】本実施形態に係る全体のシステム、鍵管理者側装置100、送信者側装置200、受信者側装置300の構成は、上述した本発明の第1実施形態のものと同様である。

【0236】以下、本システムが行う準備処理、鍵配送処理、そして暗復号化処理の3つの処理について説明する。

【0237】では、まず、準備処理について説明する。

【0238】（1）準備処理

① 送信者Aは、送信者側装置200内の乱数生成器201、素数生成器202、べき乗算器203、剰余演算器204、および演算装置205を用いて、次の情報を作成し、そのうち、公開情報のみを公開する。

【0239】秘密情報：

【0240】

【数145】

数145

$$P_A, Q_A : \text{素数}$$

$$L_A = \mathrm{lcm}(\mathrm{ord}_{P_A}(g_A), \mathrm{ord}_{Q_A}(g_A))$$

$$g_A \in \mathbb{Z}, \quad 0 < g_A < N_A$$

【0241】公開情報：

【0242】

【数146】

数146

$$N_A(=P_AQ_A)$$

【0243】秘密情報はメモリ206に格納する。また、秘密情報g_A、L_Aを通信装置207を用いて鍵管理者に送信する。

【0244】②信頼できる鍵管理者は、鍵管理者側装置100内の演算装置105を用いて、次の情報を作成する。

【0245】鍵管理者秘密情報：

【0246】

【数147】

数147

$$\bullet\ e_i \in \mathbb{Z}\ (1 \le i \le m)$$

【0247】送信者Aの送信者識別情報：

数150

$$S_{km} = \{\sigma \mid 1\text{対}1\text{写像}\ \sigma : A = \{1,2,\cdots,k\} \to B = \{1,2,\cdots,m\}, 0 < k < m\}$$

【0248】

【数148】

数148

$$\bullet\ t_A \in \mathbb{Z},\quad 0 < t_A < L_A$$

【0249】受信者xの受信者秘密情報：

【0250】

【数149】

数149

$$\bullet\ s_x(\sigma_x) \in \mathbb{Z},\quad 0 < t_A < L_A$$

【0251】これらは、σ_Xとともに全てメモリ106に格納する。

【0252】ただし、集合

【0253】

【数150】

【0254】に対して、σ、σ'∈S_{km}のとき、

【0255】

【数151】

数151

$$\sigma \sim \sigma' \quad \overset{\text{def}}{\Longleftrightarrow} \quad \sigma(A) = \sigma'(A)$$

【0256】とする。このとき、～はS_{km}上の同値関係となり、

【0257】

【数152】

数152

$$\tilde{S}_{km} = S_{km} / \sim$$

【0258】とする。

【0259】また、鍵管理者は、メモリ106から受信者秘密情報$s_X(\sigma_X)$を取り出し、σ_Xとともに受信者側携帯装置306に格納し、これを受信者xにオフラインで配布する。もちろん、他の方法によって受信者に配布するようにしてもよい。

【0260】次に、鍵配送処理について説明する。

【0261】（2）鍵配送処理

①鍵管理者は、鍵管理者側装置100内の剰余演算器104、演算装置105を用いて、送信者Aから受信したL_Aと、鍵管理者秘密情報e_iと、受信者秘密情報σ_X、$s_X(\sigma_X)$と、送信者識別情報t_Aから、

【0262】

【数153】

数153

$$\rho_x(\sigma_x(i), A) = t_A\, s_x(\sigma_x)\, e_{\sigma_x(i)} \bmod L_A \quad (1 \le i \le k)$$

【0263】なる受信者xの受信者識別データρ_X（σ_X（i），A）を計算し、通信装置107を用いて送信者Aに送信する。

【0264】また、鍵管理者は、鍵管理者側装置100内のべき乗算器103、剰余演算器104、演算装置105を用いて、送信者Aから受信したg_Aと、送信者Aの送信者公開情報N_Aと、鍵管理者秘密情報e_iから、

【0265】

【数154】

数154

$$y_{Ai} = g_A^{t_A e_i} \bmod N_A \quad (1 \le i \le m)$$

【0266】なる送信者Aの送信者鍵配送データy_{Ai}を計算し、通信装置107を用いて送信者Aに送信する。

【0267】②送信者Aは、送信者側装置200内の乱数生成器201により、乱数r、r'を作成しメモリ206に格納する。さらに、べき乗算器203、剰余演算器204、演算装置205を用いて、この乱数r、r'と、自身の秘密情報g_Aと、自身の公開情報N_Aから、

【0268】
【数155】
数155

$$K_A = g_A^{rr'} \mod N_A$$

【0269】なるデータ暗号化鍵K_Aを計算してメモリ206に格納し、受信者xとの間で鍵K_Aを共有することを目的として、剰余演算器204、演算装置205を用いて、自身の秘密情報L_Aと、乱数r'と、鍵管理者から受信した受信者xの受信者識別データρ_X（σ_X（i），A）から、
【0270】
【数156】
数156

$$\sum_{i=1}^{k} r_x(\sigma_x(i), A)\,\rho_x(\sigma_x(i), A) \equiv r' (\mathrm{mod}\, L_A)$$

【0271】なる受信者xの受信者識別情報r_X（σ_X（i），A）を計算し、通信装置207を用いて受信者xに送信する。
【0272】また、送信者Aは、送信者側装置200内のべき乗算器203、剰余演算器204、演算装置205を用いて、自身の公開情報N_Aと、乱数rと、鍵管理者から受信した送信者鍵配送データy_{Ai}から、
【0273】
【数157】
数157

$$z_{Ai} = y_{Ai}^{r} \bmod N_A \quad (1 \le i \le m)$$

【0274】なる受信者鍵配送データz_{Ai}を計算し、通信装置207を用いて受信者に同報送信する。
【0275】ここで、以上の処理において、r_X（σ_X（i），A）、z_{Ai}を作成する処理の一部を、鍵管理者が行う理由の一つは、送信者Aに対して、受信者xの受信者秘密情報σ_X、s_X（σ_X）、送信者識別番号t_Aを秘密にすることにより、送信者Aの不正を防止するためである。
【0276】❷受信者xは、送信者Aから受信した鍵配送データz_{Ai}および受信者識別情報r_X（σ_X（i），A）、鍵管理者から配送された受信者秘密情報σ_X、s_X（σ_X）、公開された送信者公開情報N_Aから、
【0277】
【数158】
数158

$$K_A = \left(\prod_{i=1}^{k} z_{A\sigma_x(i)}^{\,r_x(\sigma_x(i),A)} \right)^{s_x(\sigma_x)} \bmod N_A$$

【0278】により、データ暗号化鍵K_Aを計算し、メモリ304に格納する。
【0279】以上の処理で、送信者Aと受信者xは鍵K_Aを共有できる。他の任意の送信者と受信者についても同様にして鍵を共有できる。また、この際、送信者Aが同報送信する受信者鍵配送データz_{Ai}は、各受信者について共通である。
【0280】また、以上の処理において、受信者xが送信者Aより受けとる鍵配送データz_{Ai}および受信者識別情報r_X（σ_X（i），A）は、受信者に対して秘密化されている送信者Aの送信者識別番号t_Aが作用したものとなっている。したがって、以上の送信者識別番号t_Aを用いる構成により、受信者xが送信者Aより受けとった鍵配送データz_{Ai}、受信者識別情報r_X（σ_X（i），A）、他の送信者Bの公開情報N_B、他の送信者Bが同報通信した鍵配送データz_{Bi}より、他の送信者Bのデータ暗号化鍵K_Bを割り出すことを、きわめて困難とすることができる。
【0281】以下、暗復号化処理について説明する。
【0282】（3）暗復号化処理
❶送信者Aは、送信者側装置200内の暗復号化装置208を用いて、鍵配送処理で作成した共通鍵K_Aにより、データPを暗号化する。そして、暗号文C＝E（K_A：P）を通信装置207を用いて受信者xに送信する。
【0283】❷受信者xは、受信者側装置300内の通信装置305を用いて暗号文Cを受信し、暗復号化装置307を用いてメモリ304に格納していた共通鍵K_Aにより暗号文Cを復号化し、データを得る。
【0284】以上、本発明の第9実施形態について説明した。
【0285】本実施形態に係る鍵配送システムにおいても、上述した第1実施形態と同様、新規参入の送信者Aは、送信者秘密情報P_A、Q_A、L_A、g_Aと、送信者公開情報N_Aを作成するだけでよい。また、受信者が持つ受信者秘密情報は、全ての送信者に対して唯一であり、新たな送信者からデータを受信したい場合に、新たな受信者秘密情報を入手する必要がない。
【0286】また、受信者識別情報r_X（σ_X（i），A）によって、任意の受信者集合に属する受信者のみとのデータ暗復号のための共通鍵の共有を可能とすることができる。また、受信者数が大きい場合であっても、共通鍵配送のために同報通信する鍵配送データz_{Ai}を、これに伴い長くする必要がない。

【０２８７】なお、以上の処理において、あらかじめ、送信者Ａが送信者秘密情報L_Aを鍵管理者に送信しておき、準備処理の段階で、鍵管理者は、送信者Ａから受信した送信者秘密鍵L_Aから、

【０２８８】

【数１５９】

数159

$$e_i \in \mathbb{Z}, \quad 0 < e_i < L_A, \quad (1 \le i \le m)$$

$$t_A \in \mathbb{Z}, \quad 0 < t_A < L_A$$

$$s_x(\sigma_x) \in \mathbb{Z}, \quad 0 < s_x(\sigma_x) < L_A$$

【０２８９】となる鍵管理者秘密情報e_i、送信者識別情報t_A、受信者秘密情報$s_X(\sigma_X)$を作成し、鍵配送処理の段階で、鍵管理者は、送信者秘密情報L_A、鍵管理者秘密情報e_i、送信者識別情報t_A、受信者秘密情報$s_X(\sigma_X)$から、

【０２９０】

【数１６０】

数160

$$\rho_x(\sigma_x(i), A) = t_A \, s_x(\sigma_x) e_{\sigma_x(i)} \bmod L_A \quad (1 \le i \le k)$$

【０２９１】によって、受信者識別データ$\rho_X(\sigma_X(i), A)$を計算するようにしてもよい。

【０２９２】次に、本発明の第１０実施形態について説明する。

【０２９３】本発明の第１０実施形態は、上記の第９実施形態において、受信者側装置３００におけるデータ暗号化鍵K_Aの計算処理の一部を、受信者側携帯装置３０６で実施するようにしたものである。本実施形態で用いる受信者側携帯装置３０６の構成は、上述した本発明の第２実施形態のものと同様である。

【０２９４】本実施形態では、（１）準備処理の段階で、鍵管理者は受信者秘密情報σ_X、$s_X(\sigma_X)$を、受信者携帯装置３０６（ＩＣカード等）に格納して、受信者ｘに配布する。

【０２９５】そして、（２）鍵配送処理において、受信者ｘは、受信者側装置３００内のメモリに格納されている鍵配送データz_{Ai}を受信者携帯装置３０６に出力する。次に、受信者携帯装置３０６内で、べき乗算器３０６４、剰余演算器３０６３を用いて、受信者秘密情報σ_X、$s_X(\sigma_X)$、鍵配送データz_{Ai}および送信者公開情報N_Aから、

【０２９６】

【数１６１】

数161

$$\xi_x(\sigma_x(i), A) = z_{A\sigma_x(i)}{}^{s_x(\sigma_x)} \bmod N_A \quad (1 \le i \le k)$$

【０２９７】を計算し、この計算結果$\xi_X(\sigma_X(i), A)$を受信者側装置３００に出力する。

【０２９８】次に、受信者側装置３００内のべき乗算器３０１、剰余演算器３０２、演算装置３０３を用いて、受信者側装置３００に出力された$\xi_X(\sigma_X(i), A)$と、メモリ３０４に格納している受信者識別鍵$r_X(\sigma_X(i), A)$および送信者公開情報N_Aから、

【０２９９】

【数１６２】

数162

$$K_A = \prod_{i=1}^{k} \xi_x(\sigma_x(i), A)^{r_x(\sigma_x(i), A)} \bmod N_A$$

【０３００】により、データ暗号化鍵K_Aを計算し、メモリ３０４に格納する。

【０３０１】このように受信者秘密情報σ_X、$s_X(\sigma_X)$が受信者側携帯装置３０６外部に出力しないようにすることにより、これが電子的複写などにより盗難されることを防ぐことができる。

【０３０２】以上、本発明の第１０実施形態について説明した。

【０３０３】次に、本発明の第１１実施形態について説明する。

【０３０４】本発明の第１１実施形態は、上記の第９実施形態において、

【０３０５】

【数１６３】

数163

$$K_A = g_A{}^{rr'} \mod N_A$$

【0306】のrの値を短時間毎に、周期毎に変更し、変更後のrを用いたz_{Ai}を周期的に同報通信することにより、送信者側装置200および受信者側装置300で計算するデータ暗復号化鍵K_Aの更新を行うものである。

【0307】また、r'の値を送信データ固有の値とすることで、送信者が同報送信するデータの識別を行うようにしたものである。すなわち、受信者xがある同報データもしくは同報データの集合を復号するために、ある送信者から得た識別鍵$r_X(\sigma_X(i), A)$はその同報データ固有のものであり、別の同報データもしくは同報データの集合を取得するためには、その送信者から別の同報データもしくは同報データの集合用の別の$r_X(\sigma_X(i), A)$を得る必要がある。

【0308】以上、本発明の第11実施形態について説明した。

【0309】次に、本発明の第12実施形態について説明する。

【0310】本発明の第12実施形態は、上記の第9実施形態において、特定の受信者の認証を行い、送信者が鍵K_Aを用いて暗号化し送信した有償のデータPに対する、鍵K_Aを共有する受信者への課金を行うものである。

【0311】すなわち、第12実施形態では、さらに、以下の処理を行う。

【0312】（1）準備処理

㉖鍵管理者は、鍵管理者側装置100内の演算装置105を用いて、予め受信者xの番号UID_Xを作成し、これを受信者秘密情報$s_X(\sigma_X)$と一緒に受信者携帯装置306内のメモリ3061に格納して配布する。また、UID_Xを、$s_X(\sigma_X)$と対応させて、鍵管理者側装置100内のメモリ106に格納しておく。

【0313】㉗送信者Aは、送信者側装置200内の演算装置205を用いて、自身の番号BID_Aを作成し、メモリ206に格納しておく。また、BID_Aを通信装置207を用いて鍵管理者に送信する。

【0314】㉘鍵管理者は、鍵管理者側装置100内の通信装置107によって送信者Aの番号BID_Aを受信し、メモリ106に送信者識別情報t_Aと対応させて格納する。

【0315】㉙受信者xは、受信者側装置300内の認証装置308を用いて、受信者秘密情報$s_X(\sigma_X)$から認証用の情報を作成し、送信者Aに送信する。

【0316】㉚送信者Aは、該認証用の情報を、送信者側装置200内の認証装置209によって確認する。

【0317】この認証の方法は、上述した本発明の第4実施形態と同様、受信者が$s_X(\sigma_X)$を知らない限り、認証が成立しない認証方法であれば、従来知られている各種認証方式を用いてかまわない（ただし、このとき、送信者は受信者秘密鍵$s_X(\sigma_X)$自体は知ることができないようにする必要がある）。

【0318】㉛さて、認証を行った後に、送信者Aは、送信者側装置200内の通信装置207を用いて、自身の番号BID_Aと受信者xの番号UID_Xを鍵管理者に送信する。

【0319】㉜鍵管理者は、鍵管理者側装置100内の演算装置105を用いて、受信した送信者番号BID_Aと受信者番号UID_Xに対応した、送信者識別鍵t_Aと受信者秘密情報$s_X(\sigma_X)$から、

【0320】

【数164】

数164

$$\rho_x(\sigma_x(i), A) = t_A\, s_x(\sigma_x)\, e_{\sigma_x(i)} \bmod L_A \quad (1 \le i \le k)$$

【0321】となる受信者識別データ$\rho_X(\sigma_X(i), A)$を計算し送信者Aに送信する。

【0322】㉝送信者Aは、送信者側装置200内の剰余演算器204、演算装置205を用いて、鍵管理者から受信した受信者識別データ$\rho_X(\sigma_X(i), A)$から、

【0323】

【数165】

数165

$$\sum_{i=1}^{k} r_x(\sigma_x(i), A)\, \rho_x(\sigma_x(i), A) \equiv r' (\bmod L_A)$$

【0324】となる受信者識別情報$r_X(\sigma_X(i), A)$を計算し、通信装置207により受信者xに送信する。その際、共通鍵K_Aによって、暗号化して配信するデータ（受信者が送信要求したデータ）が有償の場合、送信者Aは、課金装置210を用いて受信者xに対して課金する。

【0325】以上、本発明の各実施形態について説明した。

【0326】なお、以上に説明した鍵管理者側装置100、送信者側装置200、受信者側装置300の各処理

は、コンピュータに各処理を実行させる手順を記述したプログラムを実行させることにより実現するようにしてもよい。この場合、各処理を実行させる手順を記述した各プログラムは、記憶媒体に格納して各コンピュータに供給するようにしてもよい。あるいは、ネットワークなどの通信媒体を介して各コンピュータに供給するようにしてもよい。

【0327】

【発明の効果】以上説明したように、本発明によれば、受信者が唯一の秘密情報によって、複数の送信者から個々の共通鍵の配送を受けることができる。また、一部の発明においては、このような鍵配送システムにおいて、任意の送信者と任意の受信者集合に属する受信者のみとのデータ暗復号のための共通鍵の共有を可能とすることができる。また、受信者数が大きい場合であっても、これに伴い共通鍵配送のための同報通信データを長くする必要がなくなる。

【図面の簡単な説明】

【図１】本発明の第１実施形態に係る鍵配送システムの構成を示すブロック図である。

【図２】本発明の第１実施形態に係る鍵管理者側装置の構成を示すブロック図である。

【図３】本発明の第１実施形態に係る送信者側装置の構成を示すブロック図である。

【図４】本発明の第１実施形態に係る受信者側装置の構成を示すブロック図である。

【図５】本発明の第１実施形態における鍵配送処理による情報の流れを示した図である。

【図６】本発明の第２実施形態に係る受信者側携帯装置の構成を示すブロック図である。

【図７】本発明の第５実施形態に係る鍵管理者側装置の構成を示すブロック図である。

【図８】本発明の第５実施形態に係る送信者側装置の構成を示すブロック図である。

【図９】本発明の第５実施形態に係る受信者側装置の構成を示すブロック図である。

【符号の説明】

１００　鍵管理者側装置

１０１、１１１、２０１、２１１、３１１　乱数生成器

１０２、２０２　素数生成器

１０３、２０３、３０１、３０６４　べき乗算器

１０４、２０４、３０２、３０６３　剰余演算器

１０５、１１２、２０５、２１２、３０３、３１２、３０６１　演算装置

１０６、１１３、２０６、２１４、３０４、３１４、３０６２　メモリ

１０７、１１４、２０７、２１５、３０５、３１５　通信装置

２００　送信者側装置

２０８、２１３、３０７、３１３　暗復号化装置

２０９、３０８　認証装置

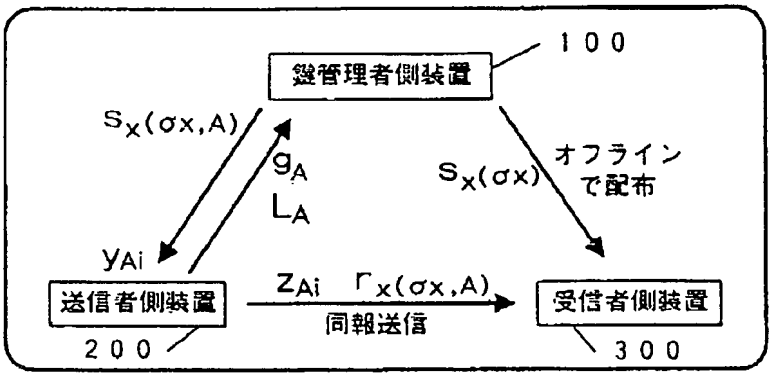
２１０　課金装置

３００　受信者側装置

３０６　受信者側携帯装置

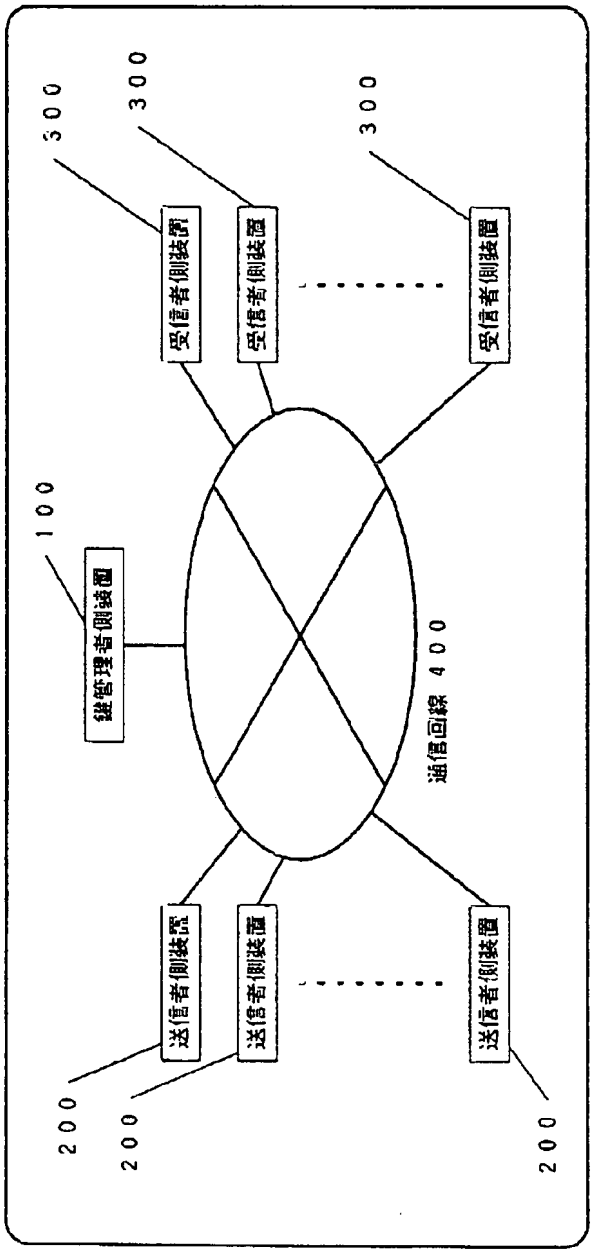
【図5】

図5



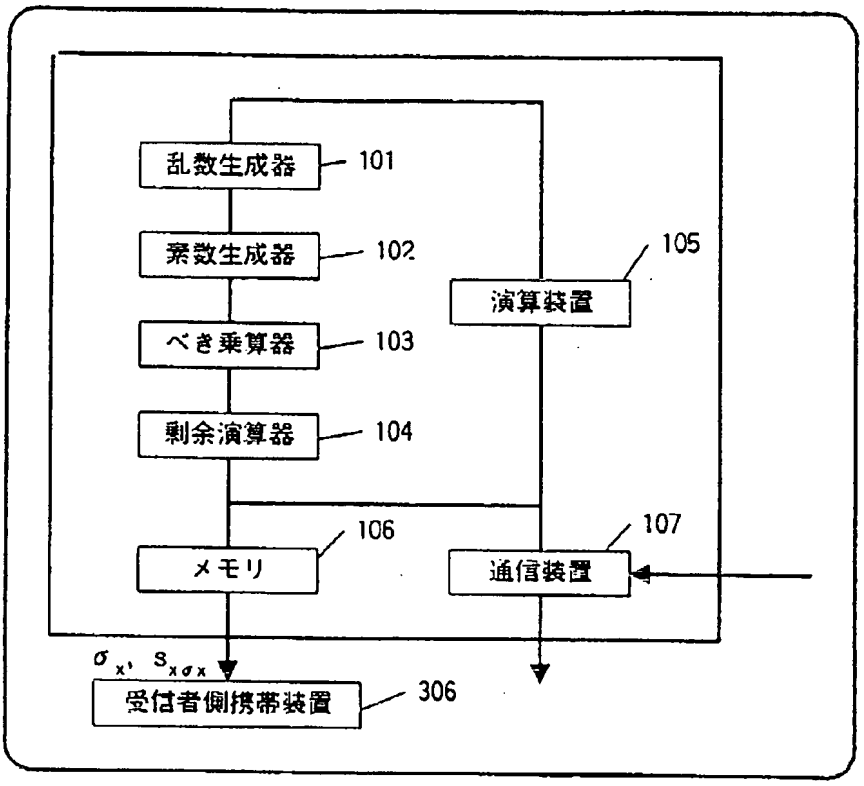
【図1】

図1


100
鍵管理者側装置
300
受信者側装置
300
受信者側装置
300
受信者側装置
通信回線 400
200
送信者側装置
200
送信者側装置
200
送信者側装置

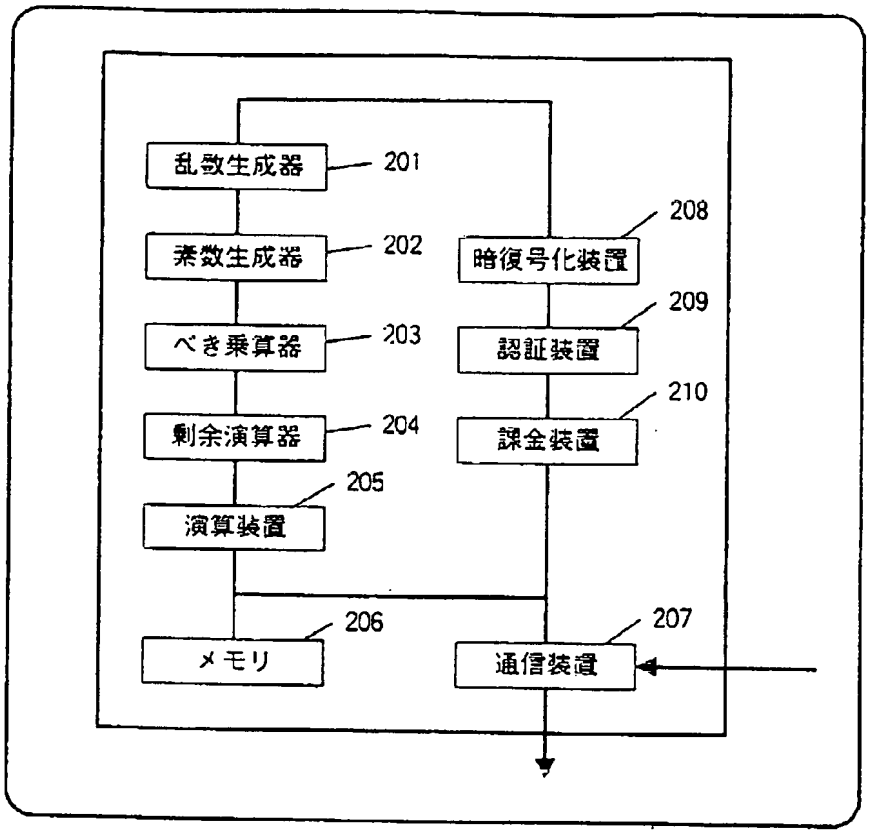
【図2】

図2


乱数生成器
101
素数生成器
102
べき乗算器
103
剰余演算器
104
メモリ
106
演算装置
105
通信装置
107
σx, Sxσx
受付者側携帯装置
306

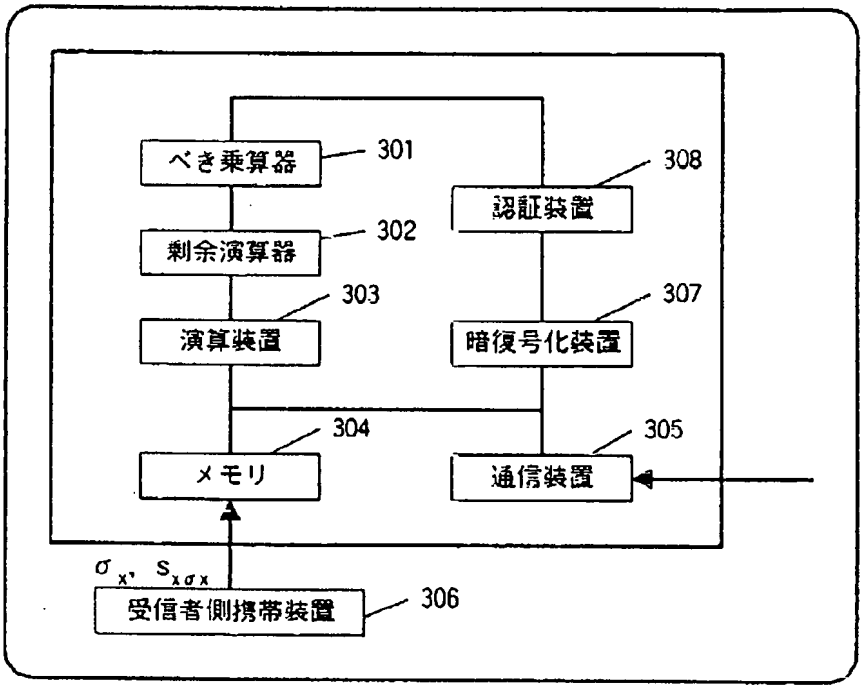
【図3】

図3


乱数生成器
201
素数生成器
202
べき乗算器
203
剰余演算器
204
演算装置
205
メモリ
206
暗復号化装置
208
認証装置
209
課金装置
210
通信装置
207

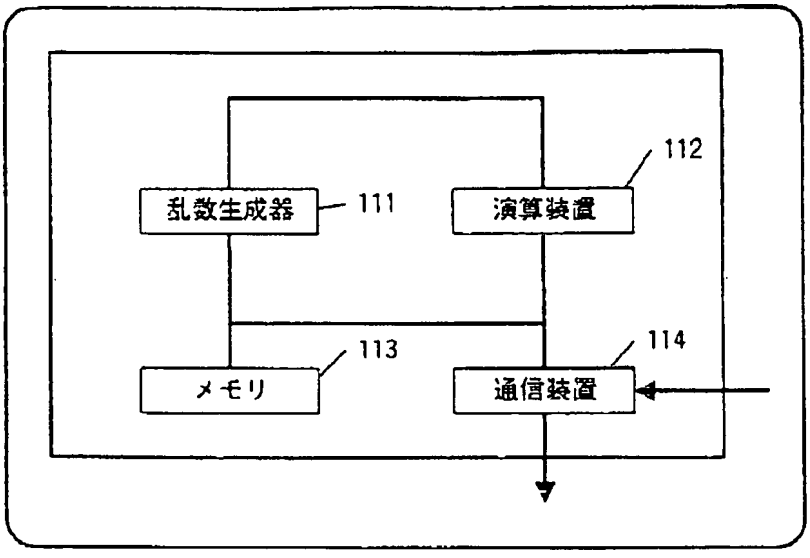
【図4】

図4


べき乗算器
301
剰余演算器
302
演算装置
303
メモリ
304
認証装置
308
暗復号化装置
307
通信装置
305
σ_x, $s_{x\sigma x}$
受信者側携帯装置
306

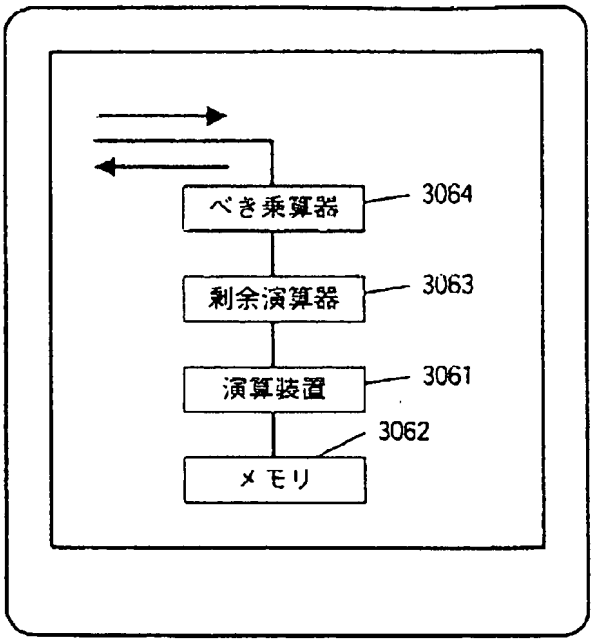
【図7】

図7


乱数生成器
111
メモリ
113
演算装置
112
通信装置
114

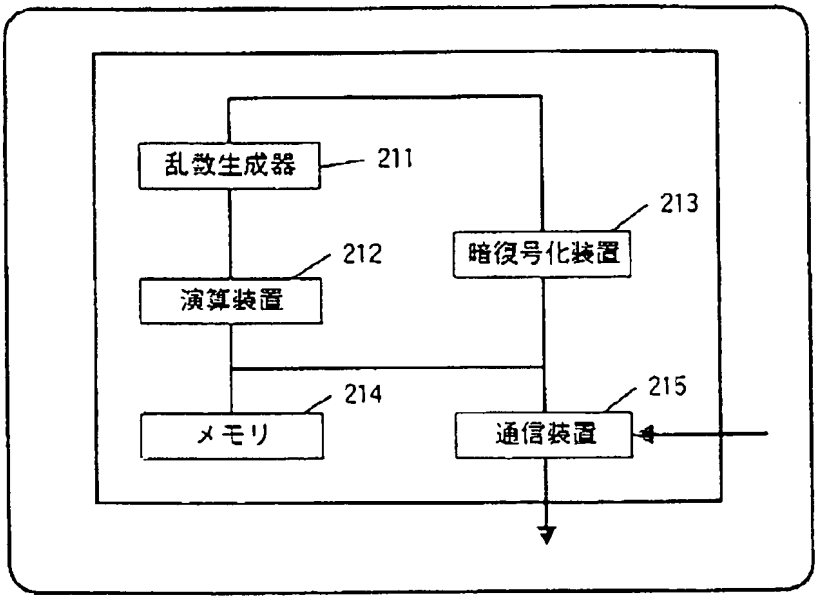
【図6】

図6


べき乗算器
3064
剰余演算器
3063
演算装置
3061
3062
メモリ

【図8】

図8


乱数生成器
211
213
暗復号化装置
212
演算装置
214
215
メモリ
通信装置

【図9】

図9